J Autom Reasoning (2017) 59:219–265
DOI 10.1007/s10817-016-9385-1

# A Complete Uniform Substitution Calculus for Differential Dynamic Logic

**André Platzer**[1]

Received: 23 December 2015 / Accepted: 29 July 2016 / Published online: 23 August 2016


**Abstract** This article introduces a relatively complete proof calculus for *differential dynamic logic* (dL) that is entirely based on *uniform substitution*, a proof rule that substitutes a formula for a predicate symbol everywhere. Uniform substitutions make it possible to use *axioms* instead of axiom schemata, thereby substantially simplifying implementations. Instead of subtle schema variables and soundness-critical side conditions on the occurrence patterns of logical variables to restrict infinitely many axiom schema instances to sound ones, the resulting calculus adopts only a finite number of ordinary dL formulas as axioms, which uniform substitutions instantiate soundly. The static semantics of differential dynamic logic and the soundness-critical restrictions it imposes on proof steps is captured exclusively in uniform substitutions and variable renamings as opposed to being spread in delicate ways across the prover implementation. In addition to sound uniform substitutions, this article introduces *differential forms* for differential dynamic logic that make it possible to internalize differential invariants, differential substitutions, and derivatives as first-class axioms to reason about differential equations axiomatically. The resulting axiomatization of differential dynamic logic is proved to be sound and relatively complete.

**Keywords** Differential dynamic logic · Uniform substitution · Axioms · Differentials · Static semantics · Axiomatization

## 1 Introduction

*Differential dynamic logic* (dL) [12,14] is a logic for proving correctness properties of hybrid systems. It has a sound and complete proof calculus relative to differential equations [12,14] and a sound and complete proof calculus relative to discrete systems [14]. Both sequent calculi [12] and Hilbert-type axiomatizations [14] have been presented for

An extended abstract has appeared at CADE [18].

✉ André Platzer
aplatzer@cs.cmu.edu

[1] Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA

dL but only the former have been implemented. The implementation of dL's sequent calculus in KeYmaera [19] makes it straightforward for users to prove properties of hybrid systems, because it provides proof rules that perform natural decompositions for each operator. The downside is that the implementation of the rule schemata and their different and subtle side conditions on occurrence constraints and relations of reading and writing of variables as well as rule applications in a formula context is quite nontrivial and inflexible in KeYmaera.

The goal of this article is to identify how to, instead, make it straightforward to implement the proof calculus of differential dynamic logic in a parsimonious way by writing down a finite list of *axioms* (concrete formulas, not axiom schemata that represent an infinite list of axioms subject to sophisticated soundness-critical schema variable matching and side condition checking implementations). The resulting calculus features more modular axioms that can be combined with one another to regain the effect of a single dL sequent proof rule. The axioms are implemented in the object language without meta constructs, which enables a substantially simpler prover core.

As a mechanism for instantiating axioms, this article follows observations for differential game logic [16] highlighting the significance and elegance of *uniform substitution*, a classical proof rule for first-order logic [2, §35, 40]. Uniform substitutions uniformly instantiate predicate and function symbols with formulas and terms, respectively, as functions of their arguments. In the presence of the nontrivial binding structure that nondeterminism and differential equations of hybrid systems induce for the dynamic modalities of differential dynamic logic, flexible but sound uniform substitutions become more complex, but can still be read off directly from the static semantics. The static semantics of dL directly determines uniform substitutions (and variable renamings), which, in turn, are the only elements of the prover core that need to know anything about the language and its static semantics. A proof may simply start from a dL formula that is an axiom.

This approach is dual to other successful ways of solving the intricacies and subtleties of substitutions [1,8] by imposing occurrence side conditions on axiom schemata and proof rules, which is what uniform substitutions get rid of. The uniform substitution framework shares many goals with other logical frameworks [11], including leading to smaller soundness-critical cores, more flexibility when augmenting reasoning techniques, and reducing the gap between a logic and its theorem prover. Logical frameworks shine when renaming and substitution of the object language are in line with those of the meta-language. Uniform substitutions provide a simpler approach for languages with the intricate binding of imperative and especially hybrid system dynamics in which, e.g., the same occurrence of a variable can be both free and bound.

Side conditions for axiom schemata can be nontrivial. Classical dL calculi [12,14] have an axiom schema expressing that a formula $\phi$ holds always after following a differential equation $x' = \theta$ (as expressed by dL formula $[x' = \theta]\phi$) iff $\phi$ holds for all times $t \geq 0$ after the discrete assignment $x := y(t)$ assigning the solution $y(t)$ to $x$:

$$([']) \quad [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi \qquad (y'(t) = \theta)$$

Soundness-critical side conditions need to ensure that $t$ is a sufficiently fresh variable and that $y(t)$ indeed solves the differential equation and obeys the symbolic initial value condition $y(0) = x$. Uniform substitutions obviate the need for such side conditions. An axiom is simply a single object-level formula as opposed to an algorithm accepting infinitely many formulas under certain side conditions. A proof rule is simply a pair of object-level formulas as opposed to an algorithm transforming formulas. Derived axioms, derived rules, rule appli-

cation mechanisms, lemmas, definitions, and parametric invariant search are all definable from uniform substitutions. *Differential forms* are added to dL in this article for the purpose of internalizing differential invariants [13], differential cuts [13,15], differential ghosts [15], differential substitutions, total differentials and Lie-derivatives [13,15] as separate first-class axioms in dL.

This article presents a highly modular and straightforward approach. It introduces *differential-form* dL and its dynamic semantics, and proves its static semantics sound for the dynamic semantics (Sect. 2). It then defines uniform substitutions that are proved sound from the static semantics (Sect. 3). Uniform substitutions enable a parsimoniously implementable axiomatization (Sect. 4) with concrete dL formulas (or pairs for rules), which are proved sound individually from the dynamic semantics (Sect. 5) without having to worry how they might be instantiated. Differential forms are used to obtain axioms for proving properties of differential equations (Sect. 5). This modular approach with separate soundness proofs is to be contrasted with previous complex built-in algorithms that mix multiple axioms into special-purpose rules [13,15]. Finally, the logic is proved to be sound and relatively complete (Sect. 5). Proofs are provided in Appendix A. Overall, uniform substitutions significantly simplify prover core implementations, because uniform substitutions are straightforward and reduce implementing axioms and axiomatic rules to copy&paste.

## 2 Differential-Form Differential Dynamic Logic

This section presents *differential-form differential dynamic logic*, which adds differential forms to differential dynamic logic [12,14] in order to axiomatically internalize reasoning about differential equations and differentials as first-class citizens. Because the logic itself did not otherwise change, the relationship to related work from previous presentations of differential dynamic logic [12,14] continues to apply. The primary purpose of the uniform substitution approach is to lead to a significantly simpler implementation, which could benefit other approaches [3,4,10], too.

### 2.1 Syntax

This section defines the syntax of the language of (differential-form) differential dynamic logic dL and its hybrid programs. The syntax first defines terms. The set of all *variables* is $\mathscr{V}$. Variables of the form $x'$ for a variable $x \in \mathscr{V}$ are called *differential symbols*. Differential symbol $x'$ is just an independent variable associated to variable $x$. For any subset $V \subseteq \mathscr{V}$ is $V' \overset{\text{def}}{=} \{x' : x \in V\}$ the set of *differential symbols* $x'$ for the variables in $V$. The set of all variables is assumed to already contain all its differential symbols $\mathscr{V}' \subseteq \mathscr{V}$. So $x \in \mathscr{V}$ implies $x', x'' \in \mathscr{V}$ etc. even if $x''$ is not used here. Function symbols are written $f, g, h$, predicate symbols $p, q, r$, and variables $x, y, z \in \mathscr{V}$ with corresponding differential symbols $x', y', z' \in \mathscr{V}'$. Program constants are $a, b, c$.

**Definition 1** *(Terms) Terms* are defined by this grammar (with $\theta, \eta, \theta_1, \ldots, \theta_k$ as terms, $x \in \mathscr{V}$ as variable, and $f$ as function symbol):

$$\theta, \eta \ ::= \ x \mid f(\theta_1, \ldots, \theta_k) \mid \theta + \eta \mid \theta \cdot \eta \mid (\theta)'$$

Number literals such as 0,1 are allowed as function symbols without arguments that are interpreted as the numbers they denote. Occasionally, constructions will be simplified by considering $\theta + \eta$ and $\theta \cdot \eta$ as special cases of function symbols $f(\theta, \eta)$, but $+$ and $\cdot$ always

denote addition and multiplication. *Differential-form* dL allows *differentials* $(\theta)'$ of terms $\theta$ as terms for the purpose of axiomatically internalizing reasoning about differential equations. The differential $(\theta)'$ describes how the value of $\theta$ changes locally depending on how the values of its variables $x$ change, i.e. as a function of the values of the corresponding differential symbols $x'$. Differentials will make it possible to reduce reasoning about *differential equations* to reasoning about *equations of differentials*, which, quite unlike differential equations, have a local semantics in isolated states and are, thus, amenable to an axiomatic treatment.

Formulas and hybrid programs (HPs) of dL are defined by simultaneous induction, because formulas can occur in programs and programs can occur in formulas. Similar simultaneous inductions are, thus, used throughout the proofs in this article.

**Definition 2** (dL*formula*) The *formulas of (differential-form) differential dynamic logic* (dL) are defined by the grammar (with dL formulas $\phi, \psi$, terms $\theta, \eta, \theta_1, \ldots, \theta_k$, predicate symbol $p$, quantifier symbol $C$, variable $x$, HP $\alpha$):

$$\phi, \psi \ ::= \ \theta \geq \eta \mid p(\theta_1, \ldots, \theta_k) \mid C(\phi) \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Operators $>, \leq, <, \vee, \rightarrow, \leftrightarrow$ are definable, e.g., $\phi \rightarrow \psi$ as $\neg(\phi \wedge \neg\psi)$. Also $[\alpha]\phi$ is equivalent to $\neg\langle\alpha\rangle\neg\phi$ and $\forall x\, \phi$ equivalent to $\neg\exists x\, \neg\phi$. The modal formula $[\alpha]\phi$ expresses that $\phi$ holds after all runs of $\alpha$, while the dual $\langle\alpha\rangle\phi$ expresses that $\phi$ holds after some run of $\alpha$. *Quantifier symbols* $C$ (with formula $\phi$ as argument), i.e. higher-order predicate symbols that bind all variables of $\phi$, are unnecessary but included for convenience since they internalize contextual congruence reasoning efficiently with uniform substitutions. The concrete quantifier chain in $\forall x\, \exists y\, \phi$ evaluates the formula $\phi$ at multiple $x$ and $y$ values to determine whether the whole formula is true. Similarly, an abstract quantifier symbol $C$ can evaluate its formula argument $\phi$ for different variable values to determine whether $C(\phi)$ is true. Whether $C(\phi)$ is true, and where exactly $C$ evaluates its argument $\phi$ to find out, depends on the interpretation of $C$.

**Definition 3** *(Hybrid program) Hybrid programs* (HPs) are defined by the following grammar (with $\alpha, \beta$ as HPs, program constant $a$, variable $x$, term $\theta$ possibly containing $x$, and with dL formula[1] $\psi$):

$$\alpha, \beta \ ::= \ a \mid x := \theta \mid ?\psi \mid x' = \theta \,\&\, \psi \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

*Assignments* $x := \theta$ of $\theta$ to variable $x$, *tests* $?\psi$ of the formula $\psi$ in the current state, *differential equations* $x' = \theta \,\&\, \psi$ restricted to the evolution domain $\psi$, *nondeterministic choices* $\alpha \cup \beta$, *sequential compositions* $\alpha; \beta$, and *nondeterministic repetition* $\alpha^*$ are as usual in dL [12,14]. The assignment $x := \theta$ instantaneously changes the value of $x$ to that of $\theta$. The test $?\psi$ checks whether $\psi$ is true in the current state and discards the program execution otherwise. The continuous evolution $x' = \theta \,\&\, \psi$ will follow the differential equation $x' = \theta$ for any nondeterministic amount of time, but cannot leave the region where the evolution domain constraint $\psi$ holds. For example, $x' = v, v' = a \,\&\, v \geq 0$ follows the differential equation where position $x$ changes with time-derivative $v$ while the velocity $v$ changes with time-derivative $a$ for any arbitrary amount of time, but without ever allowing a negative velocity $v$ (which would, otherwise, ultimately happen for negative accelerations $a < 0$). Usually, the value of differential symbol $x'$ is unrelated to the value of variable $x$. But along a differential equation $x' = \theta$, differential symbol $x'$ has the value of the time-derivative of the value of $x$ (and is, furthermore, equal to $\theta$). Differential equations $x' = \theta \,\&\, \psi$ have to be

[1] Quantifier-free formulas of first-order logic of real arithmetic are enough for most purposes.

in explicit form, so $y'$ and $(\eta)'$ cannot occur in $\theta$ and $x \notin \mathscr{V}'$. The nondeterministic choice $\alpha \cup \beta$ either executes subprogram $\alpha$ or $\beta$, nondeterministically. The sequential composition $\alpha; \beta$ first executes $\alpha$ and then, upon completion of $\alpha$, runs $\beta$. The nondeterministic repetition $\alpha^*$ repeats $\alpha$ any number of times, nondeterministically.

The effect of an assignment $x' := \theta$ to differential symbol $x' \in \mathscr{V}$, called *differential assignment*, is like the effect of an assignment $x := \theta$ to variable $x$, except that it changes the value of the differential symbol $x'$ instead of the value of $x$. It is not to be confused with the differential equation $x' = \theta$, which will follow said differential equation continuously for an arbitrary amount of time. The differential assignment $x' := \theta$, instead, only assigns the value of $\theta$ to the differential symbol $x'$ discretely once at an instant of time. Program constants $a$ are uninterpreted, i.e. their behavior depends on the interpretation in the same way that the values of function symbols $f$, predicate symbols $p$, and quantifier symbols $C$ depend on their interpretation.

*Example 4 (Simple car)* The dL formula

$$v \geq 2 \wedge b > 0 \rightarrow [((a := -b \cup a := 5);\ x' = v, v' = a \,\&\, v \geq 0)^*]\, v \geq 0 \tag{1}$$

expresses that a car starting with velocity $v \geq 2$ and braking constant $b > 0$ will always have nonnegative velocity $v \geq 0$ when following a HP that repeatedly provides a nondeterministic control choice between putting the acceleration $a$ to braking ($a := -b$) or to a positive constant ($a := 5$) before following the differential equation system $x' = v, v' = a$ restricted to the evolution domain constraint $v \geq 0$ for any amount of time. The formula in (1) is true, because the car never moves backward in the HP. But similar questions quickly become challenging, e.g., about safe distances to other cars or for models with more detailed physical dynamics.

## 2.2 Dynamic Semantics

The (denotational) dynamic semantics of dL defines, depending on the values of the symbols, what real value terms evaluate to, what truth-value formulas have, and from what initial states which final states are reachable by running its HPs. Since the values of variables and differential symbols can change over time, they receive their value by the state. A *state* is a mapping $\nu : \mathscr{V} \to \mathbb{R}$ from variables $\mathscr{V}$ including differential symbols $\mathscr{V}' \subseteq \mathscr{V}$ to $\mathbb{R}$. The set of states is denoted $\mathscr{S}$. The set $X^{\complement} = \mathscr{S} \setminus X$ is the complement of a set $X \subseteq \mathscr{S}$. Let $\nu_x^r$ denote the state that agrees with state $\nu$ except for the value of variable $x$, which is changed to $r \in \mathbb{R}$. The interpretation of a function symbol $f$ of arity $n$ (i.e. with $n$ arguments) in *interpretation* $I$ is a (smooth, i.e. with derivatives of any order) function $I(f) : \mathbb{R}^n \to \mathbb{R}$ of $n$ arguments (continuously differentiable suffices). The set of interpretations is denoted $\mathscr{I}$. The semantics of a term $\theta$ is a mapping $[\![\theta]\!] : \mathscr{I} \to (\mathscr{S} \to \mathbb{R})$ from interpretations and states to a real number.

**Definition 5** *(Semantics of terms)* The *semantics of a term* $\theta$ in interpretation $I$ and state $\nu \in \mathscr{S}$ is its value $I\nu[\![\theta]\!]$ in $\mathbb{R}$. It is defined inductively as follows

1. $I\nu[\![x]\!] = \nu(x)$ for variable $x \in \mathscr{V}$
2. $I\nu[\![f(\theta_1, \ldots, \theta_k)]\!] = I(f)\big(I\nu[\![\theta_1]\!], \ldots, I\nu[\![\theta_k]\!]\big)$ for function symbol $f$
3. $I\nu[\![\theta + \eta]\!] = I\nu[\![\theta]\!] + I\nu[\![\eta]\!]$
4. $I\nu[\![\theta \cdot \eta]\!] = I\nu[\![\theta]\!] \cdot I\nu[\![\eta]\!]$
5. $I\nu[\![(\theta)']\!] = \sum_{x \in \mathscr{V}} \nu(x') \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) = \sum_{x \in \mathscr{V}} \nu(x') \frac{\partial I\nu[\![\theta]\!]}{\partial x}$

Time-derivatives are undefined in an isolated state $\nu$. The clou is that differentials can, nevertheless, be given a local semantics in a single state: $I\nu[\![(\theta)']\!]$ is the sum of all (analytic) spatial partial derivatives at $\nu$ of the value of $\theta$ by all variables $x$ multiplied by the corresponding direction described by the value $\nu(x')$ of differential symbol $x'$. That sum over all variables $x \in \mathscr{V}$ is finite, because $\theta$ only mentions finitely many variables $x$ and the partial derivative by variables $x$ that do not occur in $\theta$ is 0. As usual, $\frac{\partial g}{\partial x}(\nu)$ is the partial derivative of function $g$ at point $\nu$ by variable $x$, which is sometimes also just denoted $\frac{\partial g(\nu)}{\partial x}$. Hence, the partial derivative $\frac{\partial I[\![\theta]\!]}{\partial x}(\nu) = \frac{\partial I\nu[\![\theta]\!]}{\partial x}$ is the derivative of the one-dimensional function $I\nu^X_x[\![\theta]\!]$ of $X$ at $\nu(x)$. The spatial partial derivatives exist since $I\nu[\![\theta]\!]$ is a composition of smooth functions, so is itself smooth. Thus, the semantics of $I\nu[\![(\theta)']\!]$ is the *differential*[2] of (the value of) $\theta$, hence a differential one-form giving a real value for each tangent vector (i.e. point of a vector field) described by the values $\nu(x')$. The values $\nu(x')$ of the differential symbols $x'$ select the direction in which $x$ changes, locally. The partial derivatives of $I\nu[\![\theta]\!]$ by $x$ describe how the value of $\theta$ changes with a change of $x$. Along the solution of (the vector field corresponding to) a differential equation, the value of differential $(\theta)'$ coincides with the analytic time-derivative of $\theta$ (Lemma 35).

The semantics of a formula $\phi$ is a mapping $[\![\phi]\!] : \mathscr{I} \to \wp(\mathscr{S})$ from interpretations to the set of all states in which $\phi$ is true, where $\wp(\mathscr{S})$ is the powerset of $\mathscr{S}$. The semantics of an HP $\alpha$ is a mapping $[\![\alpha]\!] : \mathscr{I} \to \wp(\mathscr{S} \times \mathscr{S})$ from interpretations to a reachability relation on states. The set of states $I[\![\phi]\!] \subseteq \mathscr{S}$ in which formula $\phi$ is true and the relation $I[\![\alpha]\!] \subseteq \mathscr{S} \times \mathscr{S}$ of HP $\alpha$ are defined by simultaneous induction as their syntax is simultaneously inductive. The interpretation of predicate symbol $p$ with arity $n$ is an $n$-ary relation $I(p) \subseteq \mathbb{R}^n$. The interpretation of quantifier symbol $C$ is a functional $I(C) : \wp(\mathscr{S}) \to \wp(\mathscr{S})$ mapping sets $M \subseteq \mathscr{S}$ of states where its argument is true to sets $I(C)(M) \subseteq \mathscr{S}$ of states where $C$ applied to that argument is then true.

**Definition 6** (dL *semantics*) The *semantics of a* dL *formula* $\phi$, for each interpretation $I$ with a corresponding set of states $\mathscr{S}$, is the subset $I[\![\phi]\!] \subseteq \mathscr{S}$ of states in which $\phi$ is true. It is defined inductively as follows

1. $I[\![\theta \geq \eta]\!] = \{\nu \in \mathscr{S} : I\nu[\![\theta]\!] \geq I\nu[\![\eta]\!]\}$
2. $I[\![p(\theta_1, \ldots, \theta_k)]\!] = \{\nu \in \mathscr{S} : (I\nu[\![\theta_1]\!], \ldots, I\nu[\![\theta_k]\!]) \in I(p)\}$
3. $I[\![C(\phi)]\!] = I(C)\big(I[\![\phi]\!]\big)$ for quantifier symbol $C$
4. $I[\![\neg\phi]\!] = (I[\![\phi]\!])^{\complement} = \mathscr{S} \setminus (I[\![\phi]\!])$
5. $I[\![\phi \wedge \psi]\!] = I[\![\phi]\!] \cap I[\![\psi]\!]$
6. $I[\![\exists x\, \phi]\!] = \{\nu \in \mathscr{S} : \nu^r_x \in I[\![\phi]\!] \text{ for some } r \in \mathbb{R}\}$
7. $I[\![\forall x\, \phi]\!] = \{\nu \in \mathscr{S} : \nu^r_x \in I[\![\phi]\!] \text{ for all } r \in \mathbb{R}\}$
8. $I[\![\langle\alpha\rangle\phi]\!] = I[\![\alpha]\!] \circ I[\![\phi]\!] = \{\nu : \omega \in I[\![\phi]\!] \text{ for some } \omega \text{ such that } (\nu, \omega) \in I[\![\alpha]\!]\}$
9. $I[\![[\alpha]\phi]\!] = I[\![\neg\langle\alpha\rangle\neg\phi]\!] = \{\nu : \omega \in I[\![\phi]\!] \text{ for all } \omega \text{ such that } (\nu, \omega) \in I[\![\alpha]\!]\}$

A dL formula $\phi$ is true at state $\nu$ in $I$, also written $I, \nu \models \phi$ iff $\nu \in I[\![\phi]\!]$. A dL formula $\phi$ is *valid in* $I$, written $I \models \phi$, iff $I[\![\phi]\!] = \mathscr{S}$, i.e. $\nu \in I[\![\phi]\!]$ for all states $\nu$. Formula $\phi$ is *valid*, written $\models \phi$, iff $I \models \phi$ for all interpretations $I$.

The relation composition operator $\circ$ in Case 8 is also used for sets which are unary relations. The interpretation of program constant $a$ is a state-transition relation $I(a) \subseteq \mathscr{S} \times \mathscr{S}$, where $(\nu, \omega) \in I(a)$ iff HP $a$ can run from initial state $\nu$ to final state $\omega$.

[2] The usual point-free abuse of notation aligns Definition 5 with its mathematical counterparts by rewriting the differential as $I[\![(\theta)']\!] = d(I[\![\theta]\!]) = \sum_{i=1}^n \frac{\partial I[\![\theta]\!]}{\partial x^i} dx^i$ when $x^1, \ldots, x^n$ are the variables in $\theta$ and their differentials $dx^i$ form the basis of the cotangent space, which, when evaluated at a point $\nu$ whose values $\nu(x')$ determine the actual tangent vector alias vector field.

**Definition 7** (*Transition semantics of* HPs) For each interpretation $I$, each HP $\alpha$ is interpreted semantically as a binary transition relation $I[\![\alpha]\!] \subseteq \mathscr{S} \times \mathscr{S}$ on states, defined inductively by

1. $I[\![a]\!] = I(a)$ for program constants $a$
2. $I[\![x := \theta]\!] = \{(\nu, \nu_x^r) : r = I\nu[\![\theta]\!]\} = \{(\nu, \omega) : \omega = \nu \text{ except } \omega(x) = I\nu[\![\theta]\!]\}$
3. $I[\![?\psi]\!] = \{(\nu, \nu) : \nu \in I[\![\psi]\!]\}$
4. $I[\![x' = \theta \,\&\, \psi]\!] = \{(\nu, \omega) : \nu = \varphi(0) \text{ on } \{x'\}^{\complement} \text{ and } \omega = \varphi(r) \text{ for some function } \varphi : [0, r] \to \mathscr{S} \text{ of some duration } r \text{ satisfying } I, \varphi \models x' = \theta \wedge \psi\}$
   where $I, \varphi \models x' = \theta \wedge \psi$ iff $\varphi(\zeta) \in I[\![x' = \theta \wedge \psi]\!]$ and $\varphi(0) = \varphi(\zeta)$ on $\{x, x'\}^{\complement}$ for all $0 \leq \zeta \leq r$ and if $\frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(\zeta)$ exists and is equal to $\varphi(\zeta)(x')$ for all $0 \leq \zeta \leq r$.
5. $I[\![\alpha \cup \beta]\!] = I[\![\alpha]\!] \cup I[\![\beta]\!]$
6. $I[\![\alpha; \beta]\!] = I[\![\alpha]\!] \circ I[\![\beta]\!] = \{(\nu, \omega) : (\nu, \mu) \in I[\![\alpha]\!], (\mu, \omega) \in I[\![\beta]\!] \text{ for some } \mu\}$
7. $I[\![\alpha^*]\!] = \big(I[\![\alpha]\!]\big)^* = \bigcup_{n \in \mathbb{N}} I[\![\alpha^n]\!]$ with $\alpha^{n+1} \equiv \alpha^n; \alpha$ and $\alpha^0 \equiv ?\mathit{true}$

where $\rho^*$ denotes the reflexive transitive closure of relation $\rho$.

The equality in $I[\![\alpha^*]\!]$ follows from the Scott-continuity of HPs [16, Lemma 3.7]. The case $I[\![x' = \theta \,\&\, \psi]\!]$ expresses that $\varphi$ solves the differential equation and satisfies $\psi$ at all times. In case $r = 0$, the only condition is that $\nu = \omega$ on $\{x'\}^{\complement}$ and $\omega(x') = I\omega[\![\theta]\!]$ and $\omega \in I[\![\psi]\!]$. Since $\nu$ and $\varphi(0)$ are only assumed to agree on the complement $\{x'\}^{\complement}$ of the set $\{x'\}$, the initial values $\nu(x')$ of differential symbols $x'$ do *not* influence the behavior of $(\nu, \omega) \in I[\![x' = \theta \,\&\, \psi]\!]$, because they may not be compatible with the time-derivatives for the differential equation, e.g. in $x' := 1; x' = 2$ with a discontinuity in $x'$. The final values $\omega(x')$ after $x' = \theta \,\&\, \psi$ will coincide with the derivatives at the final state, though, even for evolutions of duration zero.

### 2.3 Static Semantics

The dynamic semantics gives a precise meaning to dL formulas and HPs but is inaccessible for effective reasoning purposes. By contrast, the static semantics of dL and HPs defines only simple aspects of the dynamics concerning the variable usage that follows more directly from the syntactic structure without running the programs or evaluating their dynamical effects. The correctness of uniform substitutions depends only on the static semantics, which identifies free variables ($\mathsf{FV}(\theta)$, $\mathsf{FV}(\phi)$, $\mathsf{FV}(\alpha)$ of terms $\theta$, formulas $\phi$ and programs $\alpha$) and bound variables ($\mathsf{BV}(\alpha)$). The static semantics first characterizes free and bound variables semantically from the dynamic semantics and subsequently shows algorithms for computing them conservatively.

**Definition 8** *(Static semantics)* The *static semantics* defines the *free variables*, which are all variables that the value of an expression depends on, as well as *bound variables*, which can change their value during the evaluation of an expression, as follows:

$$\mathsf{FV}(\theta) = \bigcup\{x \in \mathscr{V} : \text{there are } I \text{ and } \nu = \tilde{\nu} \text{ on } \{x\}^{\complement} \text{ such that } I\nu[\![\theta]\!] \neq I\tilde{\nu}[\![\theta]\!]\}$$

$$\mathsf{FV}(\phi) = \bigcup\{x \in \mathscr{V} : \text{there are } I \text{ and } \nu = \tilde{\nu} \text{ on } \{x\}^{\complement} \text{ such that } \nu \in I[\![\theta]\!] \not\ni \tilde{\nu}\}$$

$$\mathsf{FV}(\alpha) = \bigcup\{x \in \mathscr{V} : \text{there are } I, \nu, \tilde{\nu}, \omega \text{ such that } \nu = \tilde{\nu} \text{ on } \{x\}^{\complement} \text{ and } (\nu, \omega) \in I[\![\alpha]\!] \text{ but there is no } \tilde{\omega} \text{ with } \omega = \tilde{\omega} \text{ on } \{x\}^{\complement} \text{ such that } (\tilde{\nu}, \tilde{\omega}) \in I[\![\alpha]\!]\}$$

$$\mathsf{BV}(\alpha) = \bigcup\{x \in \mathscr{V} : \text{there are } I \text{ and } (\nu, \omega) \in I[\![\alpha]\!] \text{ such that } \nu(x) \neq \omega(x)\}$$

The *signature*, i.e. set of function, predicate, quantifier symbols, and program constants in $\phi$ is denoted $\Sigma(\phi)$; accordingly $\Sigma(\theta)$ for term $\theta$ and $\Sigma(\alpha)$ for program $\alpha$.

For example, only $\{v, b, x\}$ are free variables of the formula (1), yet $\{a, x, x', v, v'\}$ are the bound variables of its program. Acceleration $a$ is not a free variable of (1), because $a$ is never actually read, as $a$ must have been written on *every* execution path before being read anywhere. No execution of the program in (1) depends on the initial value of $a$, so $a$ is not free since $a$ is not free after the loop or in the postcondition.

The static semantics provides uniform substitutions with all they need to know to determine what changes during substitutions go unnoticed (only changes to free variables have an impact on the value of an expression Lemma 10–12) and what state-change an expression may cause itself (only bound variables can change their value during the evaluation of an expression Lemma 9). Whether a uniform substitution preserves truth in a proof depends on the interaction of the free and bound variables. If it introduces a free variable into a context where that variable is bound, then the possible change in value of that bound variable may affect the overall truth-value.

The first property that uniform substitutions depend on is that HPs have bounded effect: only bound variables of HP $\alpha$ are modified during runs of $\alpha$.

**Lemma 9** (Bound effect) *The set* $\mathsf{BV}(\alpha)$ *is the smallest set with the bound effect property: If* $(\nu, \omega) \in I[\![\alpha]\!]$*, then* $\nu = \omega$ *on* $\mathsf{BV}(\alpha)^{\complement}$.

With a small-step operational semantics, a corresponding notion of bound variables of a formula could be defined as those that change their value during the evaluation of formulas, but that is not needed here.

The value of a term only depends on the values of its free variables. When evaluating a term $\theta$ in two different states $\nu$, $\tilde{\nu}$ that agree on its free variables $\mathsf{FV}(\theta)$, the values of $\theta$ in both states coincide. Accordingly, the value of a term will agree for different interpretations $I$, $J$ that agree on the symbols $\Sigma(\theta)$ that occur in $\theta$.

**Lemma 10** (Coincidence for terms) *The set* $\mathsf{FV}(\theta)$ *is the smallest set with the coincidence property for* $\theta$*: If* $\nu = \tilde{\nu}$ *on* $\mathsf{FV}(\theta)$ *and* $I = J$ *on* $\Sigma(\theta)$*, then* $I\nu[\![\theta]\!] = J\tilde{\nu}[\![\theta]\!]$.

In particular, the semantics of differentials is a sum over just the free variables:

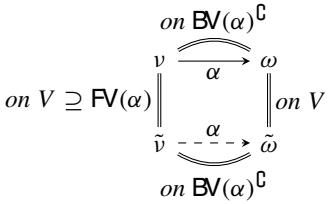
$$I\nu[\![(\theta)']\!] = \sum_{x \in \mathsf{FV}(\theta)} \nu(x') \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) = \sum_{x \in \mathsf{FV}(\theta)} \nu(x') \frac{\partial I\nu[\![\theta]\!]}{\partial x}$$

When evaluating a dL formula $\phi$ in two different states $\nu$, $\tilde{\nu}$ that agree on its free variables $\mathsf{FV}(\phi)$ in $I = J$ on $\Sigma(\phi)$, the truth-values of $\phi$ in both states coincide.

**Lemma 11** (Coincidence for formulas) *The set* $\mathsf{FV}(\phi)$ *is the smallest set with the coincidence property for* $\phi$*: If* $\nu = \tilde{\nu}$ *on* $\mathsf{FV}(\phi)$ *and* $I = J$ *on* $\Sigma(\phi)$*, then* $\nu \in I[\![\phi]\!]$ *iff* $\tilde{\nu} \in J[\![\phi]\!]$.

The runs of an HP $\alpha$ only depend on the values of its free variables, because its behavior cannot depend on the values of variables that it never reads. If $\nu = \tilde{\nu}$ on $\mathsf{FV}(\alpha)$ and $I = J$ on $\Sigma(\phi)$ and $(\nu, \omega) \in I[\![\alpha]\!]$, then there is an $\tilde{\omega}$ such that $(\tilde{\nu}, \tilde{\omega}) \in J[\![\alpha]\!]$ and $\omega$ and $\tilde{\omega}$ agree on $\mathsf{FV}(\alpha)$. In fact, the final states $\omega, \tilde{\omega}$ continue to agree on any set $V \supseteq \mathsf{FV}(\alpha)$ that the initial states $\nu$, $\tilde{\nu}$ agreed on. The respective pairs of initial and final states of a run of HP $\alpha$ already agree on the complement $\mathsf{BV}(\alpha)^{\complement}$ by Lemma 9.

**Lemma 12** (Coincidence for programs) *The set* $\mathsf{FV}(\alpha)$ *is the smallest set with the coincidence property for* $\alpha$*: If* $\nu = \tilde{\nu}$ *on* $V \supseteq \mathsf{FV}(\alpha)$*,* $I = J$ *on* $\Sigma(\alpha)$ *and* $(\nu, \omega) \in I[\![\alpha]\!]$*, then there is a* $\tilde{\omega}$ *such that* $(\tilde{\nu}, \tilde{\omega}) \in J[\![\alpha]\!]$ *and* $\omega = \tilde{\omega}$ *on* $V$*.*




## 2.4 Correct Static Semantics Computations

Lemmas 9–12 hold for any superset of $\mathsf{BV}(\alpha)$, $\mathsf{FV}(\theta)$, $\mathsf{FV}(\phi)$, $\mathsf{FV}(\alpha)$, respectively. Supersets of the static semantics can be computed easily from the syntactic structure and provide the sole input that uniform substitutions depend on, which, in turn, are the only part of the calculus where the static semantics is relevant. Only variables that are read in a formula or program can be free variables. And only variables that have quantifiers or are written to or have differential equations can be bound variables.

Bound variables $x$ of a formula are those that are bound by $\forall x$ or $\exists x$ , but also those that are bound by modalities such as $[x := 5y]$ or $\langle x' = 1\rangle$ or $[x := 1 \cup x' = 1]$ or $[x := 1 \cup ?true]$ because of the assignment to $x$ or differential equation for $x$ they contain. The scope of the bound variable $x$ is limited to the quantified formula or to the postcondition and remaining program of a modality.

**Definition 13** *(Bound variable)* The set $\mathrm{BV}(\phi) \subseteq \mathscr{V}$ of (syntactically) *bound variables* of dL formula $\phi$ is defined inductively as:

$$\begin{aligned}
\mathrm{BV}(p(\theta_1, \ldots, \theta_k)) &= \emptyset && \text{where } p \text{ can also be } \geq\\
\mathrm{BV}(C(\phi)) &= \mathscr{V}\\
\mathrm{BV}(\neg\phi) &= \mathrm{BV}(\phi)\\
\mathrm{BV}(\phi \wedge \psi) &= \mathrm{BV}(\phi) \cup \mathrm{BV}(\psi)\\
\mathrm{BV}(\forall x\, \phi) = \mathrm{BV}(\exists x\, \phi) &= \{x\} \cup \mathrm{BV}(\phi)\\
\mathrm{BV}([\alpha]\phi) = \mathrm{BV}(\langle\alpha\rangle\phi) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\phi)
\end{aligned}$$

The set $\mathrm{BV}(\alpha) \subseteq \mathscr{V}$ of (syntactically) *bound variables* of HP $\alpha$, i.e. all those that may potentially be written to, is defined inductively as:

$$\begin{aligned}
\mathrm{BV}(a) &= \mathscr{V} && \text{for program constant } a\\
\mathrm{BV}(x := \theta) &= \{x\}\\
\mathrm{BV}(?\psi) &= \emptyset\\
\mathrm{BV}(x' = \theta \,\&\, \psi) &= \{x, x'\}\\
\mathrm{BV}(\alpha \cup \beta) = \mathrm{BV}(\alpha; \beta) &= \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta)\\
\mathrm{BV}(\alpha^*) &= \mathrm{BV}(\alpha)
\end{aligned}$$

Both $x$ and $x'$ are bound by a differential equation $x' = \theta$, as both may change their value. All variables $\mathscr{V}$ is the only option for program constants and quantifier symbols $C$, since, depending on their interpretation, both may change the value of any $x \in \mathscr{V}$.

The free variables of a quantified formula are defined by removing its bound variable as $\mathrm{FV}(\forall x\, \phi) = \mathrm{FV}(\phi) \setminus \{x\}$, since all occurrences of $x$ in $\phi$ are bound by $\forall x$. The bound variables of a program in a modality act in a similar way, except that the program itself may read variables during the computation, so its free variables need to be taken into account. By analogy to the quantifier case, it is often suspected that $\mathrm{FV}([\alpha]\phi)$ could be defined as $\mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{BV}(\alpha))$. But that would be unsound, because $[x := 1 \cup y := 2]\, x \geq 1$ would have no free variables then, contradicting the fact that its truth-value depends on the initial value of $x$. The reason is that $x$ is a bound variable of that program, but only written to on some but not on all paths. So the initial value of $x$ may be needed to evaluate the truth of the postcondition $x \geq 1$ on some execution paths. If a variable is must-bound, so written to on all paths of the program, however, it can safely be removed from the free variables of the postcondition. The static semantics defines the subset of variables that are must-bound ($\mathrm{MBV}(\alpha)$), so must be written to on all execution paths of $\alpha$. This complication does not happen for ordinary quantifiers or strictly nested languages like pure $\lambda$-calculi.

**Definition 14** *(Must-bound variable)* The set $\mathrm{MBV}(\alpha) \subseteq \mathrm{BV}(\alpha) \subseteq \mathscr{V}$ of (syntactically) *must-bound variables* of HP $\alpha$, i.e. all those that must be written to on all paths of $\alpha$, is defined inductively as:

$$
\begin{aligned}
\mathrm{MBV}(a) &= \emptyset && \text{for program constant } a\\
\mathrm{MBV}(\alpha) &= \mathrm{BV}(\alpha) && \text{for atomic HPs } \alpha \text{ except program constants}\\
\mathrm{MBV}(\alpha \cup \beta) &= \mathrm{MBV}(\alpha) \cap \mathrm{MBV}(\beta)\\
\mathrm{MBV}(\alpha; \beta) &= \mathrm{MBV}(\alpha) \cup \mathrm{MBV}(\beta)\\
\mathrm{MBV}(\alpha^*) &= \emptyset
\end{aligned}
$$

Finally, the static semantics also defines which variables are free so may be read. The definition of free variables is simultaneously inductive for formulas ($\mathrm{FV}(\phi)$) and programs ($\mathrm{FV}(\alpha)$) owing to their mutually recursive syntactic structure.

**Definition 15** *(Free variable)* The set $\mathrm{FV}(\theta) \subseteq \mathscr{V}$ of (syntactically) *free variables* of term $\theta$, i.e. those that occur in $\theta$ directly or indirectly, is defined inductively as:

$$
\begin{aligned}
\mathrm{FV}(x) &= \{x\} && \text{hence } \mathrm{FV}(x') = \{x'\}\\
\mathrm{FV}(f(\theta_1, \ldots, \theta_k)) &= \mathrm{FV}(\theta_1) \cup \cdots \cup \mathrm{FV}(\theta_k) && \text{where } f \text{ can also be } + \text{ or } \cdot\\
\mathrm{FV}((\theta)') &= \mathrm{FV}(\theta) \cup \mathrm{FV}(\theta)'
\end{aligned}
$$

The set $\mathrm{FV}(\phi)$ of (syntactically) *free variables* of dL formula $\phi$, i.e. all that occur in $\phi$ outside the scope of quantifiers or modalities binding it, is defined inductively as:

$$
\begin{aligned}
\mathrm{FV}(p(\theta_1, \ldots, \theta_k)) &= \mathrm{FV}(\theta_1) \cup \cdots \cup \mathrm{FV}(\theta_k) && \text{where } p \text{ can also be } \geq\\
\mathrm{FV}(C(\phi)) &= \mathscr{V}\\
\mathrm{FV}(\neg\phi) &= \mathrm{FV}(\phi)\\
\mathrm{FV}(\phi \wedge \psi) &= \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi)\\
\mathrm{FV}(\forall x\, \phi) = \mathrm{FV}(\exists x\, \phi) &= \mathrm{FV}(\phi) \setminus \{x\}\\
\mathrm{FV}([\alpha]\phi) = \mathrm{FV}(\langle\alpha\rangle\phi) &= \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{MBV}(\alpha))
\end{aligned}
$$

The set $\mathrm{FV}(\alpha) \subseteq \mathscr{V}$ of (syntactically) *free variables* of HP $\alpha$, i.e. all those that may potentially be read, is defined inductively as:

$$\begin{aligned}
\mathrm{FV}(a) &= \mathscr{V} && \text{for program constant } a\\
\mathrm{FV}(x := \theta) &= \mathrm{FV}(\theta)\\
\mathrm{FV}(?\psi) &= \mathrm{FV}(\psi)\\
\mathrm{FV}(x' = \theta \,\&\, \psi) &= \{x\} \cup \mathrm{FV}(\theta) \cup \mathrm{FV}(\psi)\\
\mathrm{FV}(\alpha \cup \beta) &= \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta)\\
\mathrm{FV}(\alpha; \beta) &= \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha))\\
\mathrm{FV}(\alpha^*) &= \mathrm{FV}(\alpha)
\end{aligned}$$

The *variables* of dL formula $\phi$, whether free or bound, are $\mathrm{V}(\phi) = \mathrm{FV}(\phi) \cup \mathrm{BV}(\phi)$. The *variables* of HP $\alpha$, whether free or bound, are $\mathrm{V}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{BV}(\alpha)$.

Soundness requires $\mathrm{FV}((\theta)')$ to be the union of $\mathrm{FV}(\theta)$ and its differential closure $\mathrm{FV}(\theta)'$ of all differential symbols corresponding to the variables in $\mathrm{FV}(\theta)$, because the value of $(xy)'$ depends on $\mathsf{FV}((xy)') = \{x, x', y, y'\}$ so the current and differential symbol values. Indeed, $(xy)'$ will turn out to equal $x'y + xy'$ (Lemma 37), which has the same set of free variables $\{x, x', y, y'\}$ for more obvious reasons. Both $x$ and $x'$ are bound in $x' = \theta \,\&\, \psi$ since both change their value, but only $x$ is added to the free variables, because the behavior can only depend on the initial value of $x$, not of that of $x'$. All variables $\mathscr{V}$ are free and bound variables for program constants $a$, because their effect depends on the interpretation $I$, so they may read and write any variable in $\mathrm{FV}(a) = \mathrm{BV}(a) = \mathscr{V}$ but possibly not on all paths, so $\mathrm{MBV}(a) = \emptyset$.

For example, $\mathrm{FV}(\phi) = \mathsf{FV}(\phi) = \{v, b, x\}$ are the free variables of the formula $\phi$ in (1), while $\mathrm{BV}(\alpha) = \mathsf{BV}(\alpha) = \{a, x, x', v, v'\}$ are the bound variables (and must-bound variables) of its program $\alpha$. This would have been different for the less precise definition $\mathrm{FV}(\alpha; \beta) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta)$. Of course [20], syntactic computations may give bigger sets, e.g., $\mathrm{FV}(x^2 - x^2) = \{x\} \neq \mathsf{FV}(x^2 - x^2) = \emptyset$ or $\mathrm{BV}(x := x) = \{x\} \neq \mathsf{BV}(x := x) = \emptyset$, or similarly when some differential equation can never be executed.

Since uniform substitutions depend on the static semantics, soundness of uniform substitutions requires the static semantics to be computed correctly. Correctness of the static semantics is easy to prove by straightforward structural induction with some attention for differential cases. There is a subtlety in the soundness proof for the free variables of programs and formulas, though. The states $\omega$ and $\tilde{\omega}$ resulting from Lemma 12 continue to agree on $\mathrm{FV}(\alpha)$ and the variables that are bound on the particular path that $\alpha$ ran for the transition $(\nu, \omega) \in I[\![\alpha]\!]$. They may disagree on variables $z$ that are neither free (so the initial states $\nu$ and $\tilde{\nu}$ have not been assumed to coincide) nor bound on the particular path that $\alpha$ took, because $z$ has not been written to.

*Example 16 (Bound variables may not agree after an* HP) Let $(\nu, \omega) \in I[\![\alpha]\!]$. It is not enough to assume $\nu = \tilde{\nu}$ only on $\mathrm{FV}(\alpha)$ in order to guarantee $\omega = \tilde{\omega}$ on $\mathrm{V}(\alpha)$ for some $\tilde{\omega}$ such that $(\tilde{\nu}, \tilde{\omega}) \in J[\![\alpha]\!]$, because $\alpha \overset{\text{def}}{\equiv} x := 1 \cup y := 2$ will force the final states to agree only on either $x$ or on $y$, whichever one was assigned to during the respective run of $\alpha$, not on both $\mathrm{BV}(\alpha) = \{x, y\}$, even though any initial states $\nu, \tilde{\nu}$ agree on $\mathrm{FV}(\alpha) = \emptyset$. This can only happen because $\emptyset = \mathrm{MBV}(\alpha) \neq \mathrm{BV}(\alpha) = \{x, y\}$.

Yet, the respective resulting states $\omega$ and $\tilde{\omega}$ still agree on the must-bound variables that are bound on *all* paths of $\alpha$, rather than just somewhere in $\alpha$. If initial states agree on (at least) all

free variables $\mathrm{FV}(\alpha)$ that HP $\alpha$ may read, then the final states continue to agree on those (even if overwritten since) as well as on all variables that $\alpha$ must write on all paths, i.e. $\mathrm{MBV}(\alpha)$. This is crucial for the soundness proof of the syntactic static semantics, because, e.g., free occurrences in $\phi$ of must-bound variables of $\alpha$ will not be free in $[\alpha]\phi$, so the initial states will not have been assumed to agree initially. It is of similar significance that the resulting states continue to agree on any superset $V \supseteq \mathrm{FV}(\alpha)$ of the free variables that the initial states agreed on.

**Lemma 17** (Soundness of static semantics) *The static semantics correctly computes supersets and, thus, Lemmas 9–12 hold for $BV(\alpha)$, $FV(\theta)$, $FV(\phi)$, $FV(\alpha)$:*

$$BV(\alpha) \supseteq \mathsf{BV}(\alpha) \quad FV(\theta) \supseteq \mathsf{FV}(\theta) \quad FV(\phi) \supseteq \mathsf{FV}(\phi) \quad FV(\alpha) \supseteq \mathsf{FV}(\alpha)$$

In particular, the final states $\omega$ and $\tilde{\omega}$ agree on $\mathrm{V}(\alpha)$ if the initial states $\nu$ and $\tilde{\nu}$ agree on $\mathrm{V}(\alpha)$ and even if the initial states only agree on $\mathrm{V}(\alpha) \setminus \mathrm{MBV}(\alpha)$.

This concludes the static semantics of dL, which computes syntactically what kind of state change formulas $\phi$ and HPs $\alpha$ may cause (captured in $\mathrm{BV}(\phi)$, $\mathrm{BV}(\alpha)$) and what part of the state their values and behavior depends on ($\mathrm{FV}(\phi)$, $\mathrm{FV}(\alpha)$). Lemma 17 will be used implicitly in the sequel when referring to Lemmas 9–12.

## 3 Uniform Substitutions

The uniform substitution rule $\mathrm{US}_1$ from first-order logic [2, §35, 40] substitutes *all* occurrences of predicate $p(\cdot)$ by a formula $\psi(\cdot)$, i.e. it replaces all occurrences of $p(\theta)$, for any (vectorial) argument term $\theta$, by the corresponding $\psi(\theta)$ simultaneously:

$$(\mathrm{US}_1)\ \frac{\phi}{\phi^{\psi(\cdot)}_{p(\cdot)}} \qquad (\mathrm{US})\ \frac{\phi}{\sigma(\phi)}$$

Soundness of rule $\mathrm{US}_1$ [16] requires all relevant substitutions of $\psi(\theta)$ for $p(\theta)$ to be *admissible*, i.e. that no $p(\theta)$ occurs in the scope of a quantifier or modality binding a variable of $\psi(\theta)$ other than the occurrences in $\theta$; see [2, §35, 40]. A precise definition of admissibility is the key ingredient and will be developed from the static semantics.

This section develops rule US as a more general and constructive definition with a precise substitution algorithm and precise admissibility conditions that allow symbols from more syntactic categories to be substituted. The dL calculus uses uniform substitutions that affect terms, formulas, and programs. A *uniform substitution* $\sigma$ is a mapping from expressions of the form $f(\cdot)$ to terms $\sigma f(\cdot)$, from $p(\cdot)$ to formulas $\sigma p(\cdot)$, from $C(\_)$ to formulas $\sigma C(\_)$, and from program constants $a$ to HPs $\sigma a$. Vectorial extensions are accordingly for uniform substitutions of other arities $k \geq 0$. Here $\cdot$ is a reserved function symbol of arity zero and $\_$ a reserved quantifier symbol of arity zero, which mark the positions where the respective argument, e.g., argument $\theta$ to $p(\cdot)$ in the formula $p(\theta)$, will end up in the replacement $\sigma p(\cdot)$ used for $p(\theta)$.

*Example 18 (Uniform substitutions with or without clashes)* The uniform substitution $\sigma = \{f \mapsto x + 1, p(\cdot) \mapsto (\cdot \neq x)\}$ substitutes all occurrences of function symbol $f$ (of arity 0) by $x + 1$ and simultaneously substitutes all occurrences of $p(\theta)$ with predicate symbol $p$ of any argument $\theta$ by the corresponding $(\theta \neq x)$. Whether that uniform substitution is sound depends on admissibility of $\sigma$ for the formula $\phi$ in US as will be defined in Definition 19. It

will turn out to be admissible (and thus sound) for

$$\text{US}\frac{[y := f]p(2y) \leftrightarrow [y := f]p(2f)}{[y := x+1]2y \neq x \leftrightarrow [y := x+1]2(x+1) \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

but will turn out to be in-admissible (and, in fact, would be unsound) for:

$$\text{clash}\lightning\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Here, $\sigma$ is not admissible, because $\sigma$ has a free variable $x$ in its replacement for $p(\cdot)$ that it introduces into a context where $x$ is bound by the modality $[x := \ldots]$, so the $x$ in replacement $\cdot \neq x$ for $p(\cdot)$ would refer to different values in the occurrences of $p$.

Figure 1 defines the result $\sigma(\phi)$ of applying to a dL formula $\phi$ the *uniform substitution* $\sigma$ that uniformly replaces all occurrences of a function $f$ by a term (instantiated with its respective argument of $f$) and all occurrences of a predicate $p$ or a quantifier $C$ symbol by a formula (instantiated with its argument) as well as of a program constant $a$ by a program. A uniform substitution can replace any number of such function, predicate, and quantifier symbols or program constants simultaneously. The notation $\sigma f(\cdot)$ denotes the replacement for $f(\cdot)$ according to $\sigma$, i.e. the value $\sigma f(\cdot)$ of function $\sigma$ at $f(\cdot)$. By contrast, $\sigma(\phi)$ denotes the result of applying $\sigma$ to $\phi$ according to Fig. 1 (likewise for $\sigma(\theta)$ and $\sigma(\alpha)$). The notation $f \in \sigma$ signifies that $\sigma$ replaces $f$, i.e. $\sigma f(\cdot) \neq f(\cdot)$. Finally, $\sigma$ is a total function when augmented with $\sigma g(\cdot) = g(\cdot)$ for all $g \notin \sigma$, so that the case $g \notin \sigma$ in Fig. 1 is subsumed by case $f \in \sigma$. Corresponding notation is used for predicate symbols, quantifier symbols, and program constants. The cases $g \notin \sigma$, $p \notin \sigma$, $C \notin \sigma$, $b \notin \sigma$ follow from the other cases but are listed explicitly for clarity. Arguments are put in for the placeholder $\cdot$ recursively by uniform substitution $\{\cdot \mapsto \sigma(\theta)\}$ in Fig. 1, which is defined since it replaces the function symbol $\cdot$ of arity 0 by $\sigma(\theta)$, or accordingly for quantifier symbol _ of arity 0.

**Definition 19** *(Admissible uniform substitution)* A uniform substitution $\sigma$ is *$U$-admissible for $\phi$* (or $\theta$ or $\alpha$, respectively) with respect to the variables $U \subseteq \mathcal{V}$ iff $\mathsf{FV}(\sigma|_{\Sigma(\phi)}) \cap U = \emptyset$, where $\sigma|_{\Sigma(\phi)}$ is the restriction of $\sigma$ that only replaces symbols that occur in $\phi$, and $\mathsf{FV}(\sigma) = \bigcup_{f\in\sigma} \mathsf{FV}(\sigma f(\cdot)) \cup \bigcup_{p\in\sigma} \mathsf{FV}(\sigma p(\cdot))$ are the *free variables* that $\sigma$ introduces. A uniform substitution $\sigma$ is *admissible for $\phi$* (or $\theta$ or $\alpha$, respectively) iff the bound variables $U$ of each operator of $\phi$ are not free in the substitution on its arguments, i.e. $\sigma$ is $U$-admissible. These admissibility conditions are listed explicitly in Fig. 1, which defines the result $\sigma(\phi)$ of applying $\sigma$ to $\phi$.

The substitution $\sigma$ is said to *clash* and its result $\sigma(\phi)$ (or $\sigma(\theta)$ or $\sigma(\alpha)$) is not defined if $\sigma$ is not admissible, in which case rule US is not applicable either. All subsequent applications of uniform substitutions are required to be defined (no clash). If a uniform substitution is admissible using the syntactic $\mathrm{FV}(\phi)$ and $\mathrm{BV}(\alpha)$ from Sect. 2.4, then it is also admissible using the static semantics $\mathsf{FV}(\phi)$ and $\mathsf{BV}(\alpha)$ from Sect. 2.3 by Lemma 17, so that the syntactic computations can be used soundly.

*Example 20 (Admissibility)* The first use of US in Example 18 is admissible, because no free variable of the substitution is introduced into a context in which that variable is bound. The second, unsound attempt in Example 18 clashes, because it is not admissible, since $x \in \mathrm{FV}(\sigma)$ but also $x \in \mathrm{BV}(x := x+1)$. Occurrences of such bound variables that result from the arguments of the predicates or functions are exempt:

$$\text{US}\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq y \leftrightarrow x+1 \neq y} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq y)\}$$

$$
\begin{array}{rcll}
\sigma(x) & = & x & \text{for variable } x \in \mathscr{V} \\
\sigma(f(\theta)) & = & (\sigma(f))(\sigma(\theta)) \overset{\text{def}}{=} \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \text{for function symbol } f \in \sigma \\
\sigma(g(\theta)) & = & g(\sigma(\theta)) & \text{for function symbol } g \notin \sigma \\
\sigma(\theta + \eta) & = & \sigma(\theta) + \sigma(\eta) & \\
\sigma(\theta \cdot \eta) & = & \sigma(\theta) \cdot \sigma(\eta) & \\
\sigma((\theta)') & = & (\sigma(\theta))' & \text{if } \sigma \text{ is } \mathscr{V}\text{-admissible for } \theta \\
\hline
\sigma(\theta \geq \eta) & \equiv & \sigma(\theta) \geq \sigma(\eta) & \\
\sigma(p(\theta)) & \equiv & (\sigma(p))(\sigma(\theta)) \overset{\text{def}}{\equiv} \{\cdot \mapsto \sigma(\theta)\}(\sigma p(\cdot)) & \text{for predicate symbol } p \in \sigma \\
\sigma(q(\theta)) & \equiv & q(\sigma(\theta)) & \text{for predicate symbol } q \notin \sigma \\
\sigma(C(\phi)) & \equiv & \sigma(C)(\sigma(\phi)) \overset{\text{def}}{\equiv} \{\_ \mapsto \sigma(\phi)\}(\sigma C(\_)) & \text{if } \sigma \text{ is } \mathscr{V}\text{-admissible for } \phi,\ C \in \sigma \\
\sigma(C(\phi)) & \equiv & C(\sigma(\phi)) & \text{if } \sigma \text{ is } \mathscr{V}\text{-admissible for } \phi,\ C \notin \sigma \\
\sigma(\neg\phi) & \equiv & \neg\sigma(\phi) & \\
\sigma(\phi \wedge \psi) & \equiv & \sigma(\phi) \wedge \sigma(\psi) & \\
\sigma(\forall x\, \phi) & = & \forall x\, \sigma(\phi) & \text{if } \sigma \text{ is } \{x\}\text{-admissible for } \phi \\
\sigma(\exists x\, \phi) & = & \exists x\, \sigma(\phi) & \text{if } \sigma \text{ is } \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) & = & [\sigma(\alpha)]\sigma(\phi) & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma(\alpha))\text{-admissible for } \phi \\
\sigma(\langle\alpha\rangle\phi) & = & \langle\sigma(\alpha)\rangle\sigma(\phi) & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma(\alpha))\text{-admissible for } \phi \\
\hline
\sigma(a) & \equiv & \sigma a & \text{for program constant } a \in \sigma \\
\sigma(b) & \equiv & b & \text{for program constant } b \notin \sigma \\
\sigma(x := \theta) & \equiv & x := \sigma(\theta) & \\
\sigma(x' = \theta \,\&\, \psi) & \equiv & x' = \sigma(\theta) \,\&\, \sigma(\psi) & \text{if } \sigma \text{ is } \{x, x'\}\text{-admissible for } \theta, \psi \\
\sigma(?\psi) & \equiv & ?\sigma(\psi) & \\
\sigma(\alpha \cup \beta) & \equiv & \sigma(\alpha) \cup \sigma(\beta) & \\
\sigma(\alpha; \beta) & \equiv & \sigma(\alpha); \sigma(\beta) & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma(\alpha))\text{-admissible for } \beta \\
\sigma(\alpha^*) & \equiv & (\sigma(\alpha))^* & \text{if } \sigma \text{ is } \mathsf{BV}(\sigma(\alpha))\text{-admissible for } \alpha
\end{array}
$$

**Fig. 1** Recursive application of uniform substitution $\sigma$

### 3.1 Uniform Substitution Lemmas

Soundness of rule US requires proving that validity is preserved when replacing symbols with their uniform substitutes. The key to its soundness proof is to relate this syntactic change to a semantic change of the interpretations such that validity of its premise in all interpretations implies validity of the premise in the semantically modified interpretation, which is then equivalent to validity of its syntactical substitute in the conclusion. The semantic substitution corresponding to (or adjoint to) $\sigma$ modifies the interpretation of function, predicate and quantifier symbols as well as program constants semantically in the same way that $\sigma$ replaces them syntactically. When $\sigma$ is admissible, the value of an expression in the adjoint interpretation agrees with the value of its uniform substitute in the original interpretation. This link to the static semantics proves the following correspondence of syntactic and semantic substitution.

Let $I^d_{\cdot}$ denote the interpretation that agrees with interpretation $I$ except for the interpretation of function symbol $\cdot$ which is changed to $d \in \mathbb{R}$. Correspondingly $I^R_{\_}$ denotes the interpretation that agrees with $I$ except that quantifier symbol $\_$ is $R \subseteq \mathscr{S}$.

**Definition 21** *(Substitution adjoints)* The *adjoint* to substitution $\sigma$ is the operation that maps $I, \nu$ to the *adjoint* interpretation $\sigma^*_\nu I$ in which the interpretation of each function symbol $f \in \sigma$, predicate symbol $p \in \sigma$, quantifier symbol $C \in \sigma$, and program constant $a \in \sigma$ is modified according to $\sigma$:

$$
\begin{aligned}
\sigma^*_\nu I(f) &: \mathbb{R} \to \mathbb{R};\ d \mapsto I^d_{\cdot}\nu[\![\sigma f(\cdot)]\!] \\
\sigma^*_\nu I(p) &= \{d \in \mathbb{R} \,:\, \nu \in I^d_{\cdot}[\![\sigma p(\cdot)]\!]\}
\end{aligned}
$$

$$\sigma_\nu^* I(C) : \wp(\mathscr{S}) \to \wp(\mathscr{S});\ R \mapsto I^R_{\_}[\![\sigma C(\_)]\!]$$
$$\sigma_\nu^* I(a) = I[\![\sigma a]\!]$$

**Corollary 22** (Admissible adjoints) *If $\nu = \omega$ on $\mathsf{FV}(\sigma)$, then $\sigma_\nu^* I = \sigma_\omega^* I$. If $\sigma$ is U-admissible for $\theta$ (or $\phi$ or $\alpha$, respectively) and $\nu = \omega$ on $U^{\complement}$, then*

$$\sigma_\nu^* I[\![\theta]\!] = \sigma_\omega^* I[\![\theta]\!] \text{ i.e. } \sigma_\nu^* I\mu[\![\theta]\!] = \sigma_\omega^* I\mu[\![\theta]\!] \text{ for all states } \mu$$
$$\sigma_\nu^* I[\![\phi]\!] = \sigma_\omega^* I[\![\phi]\!]$$
$$\sigma_\nu^* I[\![\alpha]\!] = \sigma_\omega^* I[\![\alpha]\!]$$

Substituting equals for equals is sound by the compositional semantics of dL. The more general uniform substitutions are still sound, because the semantics of uniform substitutes of expressions agrees with the semantics of the expressions themselves in the adjoint interpretations. The semantic modification of adjoint interpretations has the same effect as the syntactic uniform substitution.

**Lemma 23** (Uniform substitution for terms) *The uniform substitution $\sigma$ and its adjoint interpretation $\sigma_\nu^* I$, $\nu$ for $I$, $\nu$ have the same semantics for all* terms $\theta$*:*

$$I\nu[\![\sigma(\theta)]\!] = \sigma_\nu^* I\nu[\![\theta]\!]$$

The uniform substitute of a formula is true at $\nu$ in an interpretation iff the formula itself is true at $\nu$ in its adjoint interpretation. Uniform substitution lemmas are proved by simultaneous induction for formulas and programs, as they are mutually recursive.

**Lemma 24** (Uniform substitution for formulas) *The uniform substitution $\sigma$ and its adjoint interpretation $\sigma_\nu^* I$, $\nu$ for $I$, $\nu$ have the same semantics for all* formulas $\phi$*:*

$$\nu \in I[\![\sigma(\phi)]\!] \text{ iff } \nu \in \sigma_\nu^* I[\![\phi]\!]$$

The uniform substitute of a program has a run from $\nu$ to $\omega$ in an interpretation iff the program itself has a run from $\nu$ to $\omega$ in its adjoint interpretation.

**Lemma 25** (Uniform substitution for programs) *The uniform substitution $\sigma$ and its adjoint interpretation $\sigma_\nu^* I$, $\nu$ for $I$, $\nu$ have the same semantics for all* programs $\alpha$*:*

$$(\nu, \omega) \in I[\![\sigma(\alpha)]\!] \text{ iff } (\nu, \omega) \in \sigma_\nu^* I[\![\alpha]\!]$$

### 3.2 Soundness

The uniform substitution lemmas are the key insights for the soundness of proof rule US, which is only applicable if its uniform substitution is defined. A proof rule is *sound* iff validity of all its premises implies validity of its conclusion.

**Theorem 26** (Soundness of uniform substitution) *The proof rule US is sound.*

$$(US)\ \frac{\phi}{\sigma(\phi)}$$

*Proof* Let the premise $\phi$ of US be valid, i.e. $\nu \in I[\![\phi]\!]$ for all interpretations and states $I, \nu$. To show that the conclusion is valid, consider any interpretation and state $I, \nu$ and show $\nu \in I[\![\sigma(\phi)]\!]$. By Lemma 24, $\nu \in I[\![\sigma(\phi)]\!]$ iff $\nu \in \sigma_\nu^* I[\![\phi]\!]$. Now $\nu \in \sigma_\nu^* I[\![\phi]\!]$ holds, because $\nu \in I[\![\phi]\!]$ for all $I, \nu$, including for $\sigma_\nu^* I, \nu$, by premise. The rule $\mathrm{US}_1$ is the special case of US where $\sigma$ only substitutes predicate symbol $p$. □

Uniform substitutions can also be used to soundly instantiate locally sound proof rules or whole proofs just like proof rule US soundly instantiates axioms or other valid formulas (Theorem 26). An inference or proof rule is *locally sound* iff its conclusion is valid in any interpretation $I$ in which all its premises are valid. All locally sound proof rules are sound. The use of Theorem 27 in a proof is marked USR.

**Theorem 27** (Soundness of uniform substitution of rules) *All uniform substitution instances (with* $\mathsf{FV}(\sigma) = \emptyset$*) of locally sound inferences are* locally sound*:*

$$\frac{\phi_1 \quad \ldots \quad \phi_n}{\psi} \text{ locally sound} \quad \text{implies} \quad \frac{\sigma(\phi_1) \quad \ldots \quad \sigma(\phi_n)}{\sigma(\psi)} \text{ locally sound}$$

*Proof* Let $\mathscr{D}$ be the inference on the left and let $\sigma(\mathscr{D})$ be the substituted inference on the right. Assume $\mathscr{D}$ to be locally sound. To show that $\sigma(\mathscr{D})$ is locally sound, consider any $I$ in which all premises of $\sigma(\mathscr{D})$ are valid, i.e. $I \models \sigma(\phi_j)$ for all $j$. That is, $\nu \in I[\![\sigma(\phi_j)]\!]$ for all $\nu$ and all $j$. By Lemma 24, $\nu \in I[\![\sigma(\phi_j)]\!]$ is equivalent to $\nu \in \sigma_\nu^* I[\![\phi_j]\!]$, which, thus, also holds for all $\nu$ and all $j$. By Corollary 22, $\sigma_\nu^* I[\![\phi_j]\!] = \sigma_\omega^* I[\![\phi_j]\!]$ for any $\omega$, since $\mathsf{FV}(\sigma) = \emptyset$. Fix an arbitrary state $\omega$. Then $\nu \in \sigma_\omega^* I[\![\sigma(\phi_j)]\!]$ holds for all $\nu$ and all $j$ for the same (arbitrary) $\omega$ that determines $\sigma_\omega^* I$.

Consequently, all premises of $\mathscr{D}$ are valid in the same $\sigma_\omega^* I$, i.e. $\sigma_\omega^* I \models \phi_j$ for all $j$. Thus, $\sigma_\omega^* I \models \psi$ by local soundness of $\mathscr{D}$. That is, $\nu \in \sigma_\nu^* I[\![\psi]\!] = \sigma_\omega^* I[\![\psi]\!]$ by Corollary 22 for all $\nu$. By Lemma 24, $\nu \in \sigma_\nu^* I[\![\psi]\!]$ is equivalent to $\nu \in I[\![\sigma(\psi)]\!]$, which continues to hold for all $\nu$. Thus, $I \models \sigma(\psi)$, i.e. the conclusion of $\sigma(\mathscr{D})$ is valid in $I$, hence $\sigma(\mathscr{D})$ is locally sound. Consequently, all uniform substitution instances $\sigma(\mathscr{D})$ of locally sound inferences $\mathscr{D}$ with $\mathsf{FV}(\sigma) = \emptyset$ are locally sound. □

If $\psi$ has a proof (i.e. $n = 0$), USR preserves local soundness even if $\mathsf{FV}(\sigma) \neq \emptyset$, because US proves $\sigma(\psi)$ from the provable $\psi$, which makes this inference locally sound, since local soundness is equivalent to soundness for $n = 0$ premises. If $\psi$ has a proof, uniform substitution of rules USR for $n = 0$ premises is identical to rule US.

*Example 28 (Uniform substitutions are only globally sound)* Rule US itself is only sound but not locally sound, so it cannot have been used on any unproved premises at any point during a proof that is to be instantiated by proof rule USR from Theorem 27. The following sound proof on the left with a modus ponens (marked MP) has an unproved premise on which US has been used at some point during the proof:

$$\dfrac{\dfrac{*}{1 = 0 \rightarrow [x' = 2]\, x < 5} \quad \text{US}\ \dfrac{f(x) = 0}{1 = 0}}{[x' = 2]\, x < 5}\ \text{MP} \qquad \text{USR not applicable} \qquad \text{clash}\lightning\ \dfrac{0 = 0}{[x' = 2]\, x < 5}$$

This use of US, which substitutes 1 for $f(\cdot)$, makes the left proof sound but *not* locally sound. That prevents rule USR of Theorem 27 from (unsoundly) concluding the uniform substitution instance on the right with $\sigma = \{f(\cdot) \mapsto 0\}$. Rule US assumes that its premise is valid (in all interpretations $I$), but the (clashing) substitution instance on the right only proves one choice for $f$ to satisfy premise $f(x) = 0$. Rule US can still be used in the proof of a premise that proves without endangering local soundness, because proved premises are valid in all interpretations by soundness.

$$\langle\cdot\rangle \quad \langle a\rangle p(\bar{x}) \leftrightarrow \neg[a]\neg p(\bar{x})$$
$$[:=] \quad [x := f]p(x) \leftrightarrow p(f)$$
$$[?] \quad [?q]p \leftrightarrow (q \rightarrow p)$$
$$[\cup] \quad [a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$$
$$[;] \quad [a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$$
$$[^*] \quad [a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a][a^*]p(\bar{x})$$
$$\mathrm{K} \quad [a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$$
$$\mathrm{I} \quad [a^*](p(\bar{x}) \rightarrow [a]p(\bar{x})) \rightarrow (p(\bar{x}) \rightarrow [a^*]p(\bar{x}))$$
$$\mathrm{V} \quad p \rightarrow [a]p$$

$$\mathrm{G} \quad \frac{p(\bar{x})}{[a]p(\bar{x})}$$
$$\forall \quad \frac{p(x)}{\forall x\, p(x)}$$
$$\mathrm{MP} \quad \frac{p \rightarrow q \quad p}{q}$$
$$\mathrm{CQ} \quad \frac{f(\bar{x}) = g(\bar{x})}{p(f(\bar{x})) \leftrightarrow p(g(\bar{x}))}$$
$$\mathrm{CE} \quad \frac{p(\bar{x}) \leftrightarrow q(\bar{x})}{C(p(\bar{x})) \leftrightarrow C(q(\bar{x}))}$$

**Fig. 2** Differential dynamic logic axioms and proof rules

## 4 Differential Dynamic Logic Axioms

Proof rules and axioms for a Hilbert-type axiomatization of dL from prior work [14] are shown in Fig. 2, except that, thanks to proof rule US, axioms and proof rules now reduce to the finite list of concrete dL formulas in Fig. 2 as opposed to an infinite collection of axioms from a finite list of axiom schemata along with schema variables, side conditions, and implicit instantiation rules. Soundness of the axioms follows from soundness of corresponding axiom schemata [7,14], but is easier to prove standalone, because it is a finite list of formulas without the need to prove soundness for all their instances. Soundness of axioms, thus, reduces to validity of one formula as opposed to validity of all formulas that can be generated by the instantiation mechanism complying with the respective side conditions for that axiom schema. The proof rules in Fig. 2 are *axiomatic rules*, i.e. pairs of concrete dL formulas to be instantiated by USR. Soundness of axiomatic rules reduces to proving that their concrete conclusion formula is a consequence of their premise formula. Further, $\bar{x}$ is the vector of all relevant variables, which is finite-dimensional, or considered as a built-in vectorial term. Proofs in the uniform substitution dL calculus use US (and variable renaming such as $\forall x\, p(x)$ to $\forall y\, p(y)$) to instantiate the axioms from Fig. 2 to the required form.

*Diamond axiom* $\langle\cdot\rangle$ expresses the duality of the $[\cdot]$ and $\langle\cdot\rangle$ modalities. *Assignment axiom* $[:=]$ expresses that $p(x)$ holds after the assignment $x := f$ iff $p(f)$ holds initially. *Test axiom* $[?]$ expresses that $p$ holds after the test $?q$ iff $p$ is implied by $q$, because test $?q$ only runs when $q$ holds. *Choice axiom* $[\cup]$ expresses that $p(\bar{x})$ holds after all runs of $a \cup b$ iff $p(\bar{x})$ holds after all runs of $a$ and after all runs of $b$. *Sequential composition axiom* $[;]$ expresses that $p(\bar{x})$ holds after all runs of $a; b$ iff, after all runs of $a$, it is the case that $p(\bar{x})$ holds after all runs of $b$. *Iteration axiom* $[^*]$ expresses that $p(\bar{x})$ holds after all repetitions of $a$ iff it holds initially and, after all runs of $a$, it is the case that $p(\bar{x})$ holds after all repetitions of $a$. Axiom K is the *modal modus ponens* from modal logic [9]. *Induction axiom* I expresses that if, no matter how often $a$ repeats, $p(\bar{x})$ holds after all runs of $a$ if it was true before, then, if $p(\bar{x})$ holds initially, it holds after all repetitions of $a$. *Vacuous axiom* V expresses that arity 0 predicate symbol $p$ continues to hold after all runs of $a$ if it was true before.

*Gödel's generalization* rule G expresses that $p(\bar{x})$ holds after all runs of $a$ if $p(\bar{x})$ is valid. Accordingly $\forall$ is the $\forall$-*generalization* rule. MP is *modus ponens*. *Congruence* rules CQ, CE are not needed but included to efficiently use axioms in any context. Congruence rule CT derives from CQ using $p(\cdot) \overset{\text{def}}{\equiv} \big(c(\cdot) = c(g(\bar{x}))\big)$ and reflexivity:

$$(\text{CT})\ \frac{f(\bar{x}) = g(\bar{x})}{c(f(\bar{x})) = c(g(\bar{x}))}$$

*Remark 29* The use of variable vector $\bar{x}$ is not essential but simplifies concepts. An equivalent axiomatization is obtained when considering $p(\bar{x})$ to be a quantifier symbol of arity 0 in the axiomatization, or as $C(\mathit{true})$ with a quantifier symbol of arity 1. Neither replacements of quantifier symbols nor (vectorial) placeholders $\cdot$ for the substitutions $\{p(\cdot) \mapsto \psi\}$ that are used for $p(\bar{x})$ cause any free variables in the substitution. The mnemonic notation $\sigma = \{p(\bar{x}) \mapsto \phi\}$ adopted for such uniform substitutions reminds that the variables $\bar{x}$ are not free in $\sigma$ even if they occur in the replacement $\phi$.

Sound axioms are just valid formulas, so true in all states. For example, in any state where $[a][b]p(\bar{x})$ is true, $[a;b]p(\bar{x})$ is true, too, by equivalence axiom [;]. Using axiom [;] to replace one by the other is a truth-preserving transformation, i.e. in any state in which one is true, the other is true, too. Sound rules are validity-preserving, i.e. the conclusion is valid if the premises are valid, which is weaker than truth-preserving transformation. For proof search, the dL axioms are meant to be used to reduce the *axiom key* (marked blue) to the structurally simpler remaining conditions (right-hand sides of equivalences and the conditions assumed in implications).

*Real Quantifiers.* Besides (decidable) real arithmetic (whose use is denoted $\mathbb{R}$), complete axioms for first-order logic can be adopted to express universal instantiation $\forall$i (if $p$ is true of all $x$, it is also true of constant function symbol $f$), distributivity $\forall\rightarrow$, and vacuous quantification $\mathrm{V}_\forall$ (predicate $p$ of arity zero does not depend on $x$).

$$(\forall\text{i})\quad (\forall x\ p(x)) \rightarrow p(f)$$
$$(\forall\rightarrow)\quad \forall x\ (p(x) \rightarrow q(x)) \rightarrow (\forall x\ p(x) \rightarrow \forall x\ q(x))$$
$$(\mathrm{V}_\forall)\quad p \rightarrow \forall x\ p$$

*The Significance of Clashes.* This section illustrates how uniform substitutions tell sound instantiations apart from unsound proof attempts. Rule US clashes exactly when the substitution introduces a free variable into a bound context, which would be unsound. Example 18 on p. 13 already showed that even an occurrence of $p(x)$ in a context where $x$ is bound does not permit mentioning $x$ in the replacement except in the $\cdot$ places. US can directly handle even nontrivial binding structures, though, e.g. from [:=] with the substitution $\sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$:

$$\text{US}\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x+z)^*; z := x+yz]\, y{\geq}x \leftrightarrow [(z := x^2+z)^*; z := x^2+yz]\, y{\geq}x^2}$$

It is soundness-critical that US clashes when trying to instantiate $p$ in $\mathrm{V}_\forall$ with a formula that mentions the bound variable $x$:

$$\text{clash}\lightning\frac{p \rightarrow \forall x\ p}{x \geq y \rightarrow \forall x\ (x \geq y)} \qquad \{p \mapsto x \geq y\}$$

It is soundness-critical that US clashes when substituting $p$ in vacuous program axiom V with a formula with a free occurrence of a variable bound by the replacement of $a$:

$$\text{clash}\lightning\frac{p \rightarrow [a]p}{x \geq y \rightarrow [x' = -1]\, x \geq y} \qquad \{a \mapsto x' = -1, p \mapsto x \geq y\}$$

Additional free variables are acceptable, though, e.g. in replacements for $p$ as long as they are not bound in the particular context into which they will be substituted:

$$\text{US}\frac{p \to [a]p}{y \geq 0 \to [x' = -1]\, y \geq 0} \qquad \{a \mapsto x' = -1,\ p \mapsto y \geq 0\}$$

Complex formulas are acceptable as replacements for $p$ if their free variables are not bound in the context, e.g., using $\sigma = \{a \mapsto x' := 5x,\ p \mapsto [x' = x^2 - 2x + 2]x \geq 1\}$:

$$\text{US}\frac{p \to [a]p}{[x' = x^2 - 2x + 2]\, x \geq 1 \to [x' := 5x][x' = x^2 - 2x + 2]\, x \geq 1}$$

But it is soundness-critical that US clashes when substituting a formula with a free dependence on $x'$ for $p$ into a context where $x'$ will be bound after the substitution:

$$\text{clash}\lightning\frac{p \to [a]p}{(x-1)' \geq 0 \to [x' := 5x](x-1)' \geq 0} \qquad \{a \mapsto x' := 5x,\ p \mapsto (x-1)' \geq 0\}$$

Gödel's generalization rule G uses $p(\bar{x})$ instead of the $p$ that V uses, so its USR instance allows all variables $\bar{x}$ to occur in the replacement without causing a clash:

$$\text{G,USR}\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \qquad \{a \mapsto x' = -1,\ p(\bar{x}) \mapsto (-x)^2 \geq 0\}$$

Intuitively, the argument $\bar{x}$ in this uniform substitution instance of G was not introduced as part of the substitution but merely put in for the placeholder $\cdot$ instead. Let $\bar{x} = (x, y)$, US $\{a \mapsto x := x + 1, b \mapsto x := 0; y' = -2,\ p(\bar{x}) \mapsto x \geq y\}$ derives from [∪]:

$$\text{US}\frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})}{[x := x+1 \cup (x := 0; y' = -2)]\, x \geq y \leftrightarrow [x := x + 1]\, x \geq y \wedge [x := 0; y' = -2]\, x \geq y}$$

With $\bar{x} = (x, y)$ and $\{a \mapsto x := x + 1 \cup y := 0, b \mapsto y' = -1, p(\bar{x}) \mapsto x \geq y\}$, US yields:

$$\text{US}\frac{[a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})}{[(x := x + 1 \cup y := 0); y' = -1]\, x \geq y \leftrightarrow [x := x + 1 \cup y := 0][y' = -1]\, x \geq y}$$

Not all axioms fit to the uniform substitution framework, though. The Barcan schema was used in a completeness proof for the Hilbert-type calculus for differential dynamic logic [14] (but not in the completeness proof for its sequent calculus [12]):

$$\text{(B)}\ \ \forall x\, [\alpha]p(x) \to [\alpha]\forall x\, p(x) \quad (x \notin \alpha)$$

Axiom schema B is unsound without the restriction $x \notin \alpha$, though, so that the following formula, which cannot enforce $x \notin a$, would be an unsound axiom

$$\forall x\, [a]p(x) \to [a]\forall x\, p(x) \tag{2}$$

Indeed, the effect of program constant $a$ might depend on the value of $x$ or it might write to $x$. In (2), $x$ cannot be written by $a$ without violating soundness:

$$\lightning\frac{\forall x\, [a]p(x) \to [a]\forall x\, p(x)}{\forall x\, [x := 0]\, x \geq y \to [x := 0]\forall x\, (x \geq y)} \qquad \{a \mapsto x := 0,\ p(\cdot) \mapsto \cdot \geq 0\}$$

nor can $x$ be read by $a$ in (2) without violating soundness:

$$\lightning\frac{\forall x\, [a]p(x) \to [a]\forall x\, p(x)}{\forall x\, [?(y = x^2)]\, y = x^2 \to [?(y = x^2)]\forall x\, y = x^2} \qquad \{a \mapsto ?(y = x^2),\ p(\cdot) \mapsto y = \cdot^2\}$$

$$\text{DW}\quad [x' = f(x)\,\&\,q(x)]q(x)$$

$$\text{DC}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

$$\text{DE}\quad [x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$$

$$\text{DI}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [?q(x)]p(x)\big) \leftarrow \big(q(x) \rightarrow [x' = f(x)\,\&\,q(x)](p(x))'\big)$$

$$\text{DG}\quad [x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)$$

$$\text{DS}\quad [x' = f\,\&\,q(x)]p(x) \leftrightarrow \forall t{\geq}0\,\big((\forall 0{\leq}s{\leq}t\; q(x+fs)) \rightarrow [x := x+ft]p(x)\big)$$

$$c'\quad (f)' = 0$$

$$x'\quad (x)' = x'$$

$$+'\quad (f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$$

$$\cdot'\quad (f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$$

$$\circ'\quad [y := g(x)][y' := 1]\big((f(g(x)))' = (f(y))' \cdot (g(x))'\big)$$

**Fig. 3** Differential equation axioms and differential axioms

Thus, the completeness proof for differential dynamic logic from prior work [14] does not carry over. A more general completeness result for differential game logic [16] implies, however, that Barcan schema B is unnecessary for completeness.

## 5 Differential Equations and Differential Axioms

Section 4 leverages uniform substitutions to obtain a finite list of axioms without side-conditions. They lack axioms for differential equations, though. Classical calculi for dL have axiom schema [′] from p. 2 for replacing differential equations with time quantifiers and discrete assignments for their solutions. In addition to being limited to simple solvable differential equations, such axiom schemata have quite nontrivial soundness-critical side conditions.

This section leverages US and the new differential forms in dL to obtain a logically internalized version of differential invariants and related proof rules for differential equations [13,15] as axioms (without schema variables or side-conditions). These axioms can prove properties of more general "unsolvable" differential equations. They can also prove all properties of differential equations that can be proved with solutions [15] while guaranteeing correctness of the solution as part of the proof.

### 5.1 Differentials: Invariants, Cuts, Effects, and Ghosts

Figure 3 shows axioms for proving properties of differential equations (DW–DS), and differential axioms for differentials $(+', \cdot', \circ')$ which are equations of differentials. Axiom $x'$ identifying $(x)' = x'$ for variables $x \in \mathcal{V}$ and axiom $c'$ for functions $f$ and number literals of arity 0 are used implicitly to save space. Some axioms use reverse implication notation $\phi \leftarrow \psi$ instead of the equivalent $\psi \rightarrow \phi$ for emphasis.

*Differential weakening* axiom DW internalizes that differential equations never leave their evolution domain $q(x)$. The evolution domain $q(x)$ holds after all evolutions of $x' = f(x)\,\&\,q(x)$, because differential equations cannot leave their evolution domains. DW derives[3] $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)](q(x) \rightarrow p(x))$, which allows to

[3] The implication $[x' = f(x)\,\&\,q(x)](q(x) \rightarrow p(x)) \rightarrow [x' = f(x)\,\&\,q(x)]p(x)$ derives by K from DW. The converse implication $[x' = f(x)\,\&\,q(x)]p(x) \rightarrow [x' = f(x)\,\&\,q(x)](q(x) \rightarrow p(x))$ derives by K since G derives $[x' = f(x)\,\&\,q(x)]\big(p(x) \rightarrow (q(x) \rightarrow p(x))\big)$ from the tautology $p(x) \rightarrow (q(x) \rightarrow p(x))$.

export the evolution domain to the postcondition and is also called DW. Its (right) assumption is best proved by G yielding premise $q(x) \rightarrow p(x)$. The *differential cut* axiom DC is a cut for differential equations. It internalizes that differential equations always staying in $r(x)$ also always stay in $p(x)$ iff $p(x)$ always holds after the differential equation that is restricted to the smaller evolution domain $\& q(x) \wedge r(x)$. DC is a differential variant of modal modus ponens axiom K.

*Differential effect* axiom DE internalizes that the effect on differential symbols along a differential equation is a differential assignment assigning the right-hand side $f(x)$ to the left-hand side $x'$. The differential assignment $x' := f(x)$ in DE instantaneously mimics the (continuous) effect that the differential equation $x' = f(x) \& q(x)$ has on $x'$, thereby selecting the appropriate vector field for subsequent differentials. Axiom DI internalizes *differential invariants* [13], i.e. that $p(x)$ holds always after a differential equation $x' = f(x) \& q(x)$ iff it holds after $?q(x)$, provided its differential $(p(x))'$ always holds after the differential equation $x' = f(x) \& q(x)$. This axiom reduces future truth to present truth when the truth of $p(x)$ does not change along the differential equation because $(p(x))'$ holds all along. The differential equation also vacuously stays in $p(x)$ if it starts outside $q(x)$, since it is stuck then. The assumption of DI is best proved by DE to select the appropriate vector field $x' = f(x)$ for the differential $(p(x))'$ and a subsequent DW, G to make the evolution domain constraint $q(x)$ available as an assumption when showing $(p(x))'$. The condition $[?q(x)]p(x)$ in DI is equivalent to $q(x) \rightarrow p(x)$ by axiom [?]. While a general account of $(p(x))'$ is possible [17], this article focuses on atomic postconditions with the equivalences $(\theta \geq \eta)' \equiv (\theta > \eta)' \equiv (\theta)' \geq (\eta)'$ and $(\theta = \eta)' \equiv (\theta \neq \eta)' \equiv (\theta)' = (\eta)'$, etc. for DI axioms. Note $(\theta \neq \eta)'$ cannot be $(\theta)' \neq (\eta)'$, because different rates of change from different initial values do not imply the values would remain different. Conjunctions can be handled separately by $[\alpha](p(\bar{x}) \wedge q(\bar{x})) \leftrightarrow [\alpha]p(\bar{x}) \wedge [\alpha]q(\bar{x})$ which derives from K. Disjunctions split into separate disjuncts, which is equivalent to classical differential invariants [13] but easier. Axiom DG internalizes *differential ghosts* [15], i.e. that additional differential equations can be added whose solutions exist long enough, which can enable new invariants that are not otherwise provable [15]. Axiom DS solves constant differential equations, and, as Sect. 5.2 will demonstrate, more complex solvable differential equations with the help of DG, DC, DI. Vectorial generalizations to systems of differential equations are possible for the axioms in Fig. 3.

The differential axioms for differentials $(+',\cdot',\circ',c',x')$ axiomatize differentials of polynomials. They are related to corresponding rules for time-derivatives, except that those would be ill-defined in a local state, so it is crucial to work with differentials that have a local semantics in individual states. Uniform substitutions correctly maintain that $y$ does not occur in replacements for $a(x)$, $b(x)$ for DG and that $x$ does not occur in replacements for $f$ in DS, which are both soundness-critical. Occurrences of $x$ in replacements for $f$ are acceptable when using axiom [:=] on $[x' := f]p(x') \leftrightarrow p(f)$.

Most axioms in Figs. 2 and 3 are independent, because there is exactly one axiom per operator. Exceptions in Fig. 2 are K, I, V, but there is a complete calculus without [*], V [14] and one without G, K, I, V that uses two extra rules instead [16]. The congruence rules CQ, CE are redundant and can be proved on a per-instance basis as well. Axiom DW is the only one that can use the evolution domain, axiom DC the only one that can change the evolution domain, and axiom DG the only one that can change differential equations. Axiom DE is the only one that can use the right-hand side of the differential equation. Axiom DI is the only axiom that relates truth of a postcondition after a differential equation to truth at the initial state. Finally, axiom DS is needed for proving diamond properties of differential equations, because it is the only one (besides the limited DW) that does not reduce a property of a

differential equation to another property of a differential equation and, thus, the only axiom that ultimately proves them without the help of G, V, K, which are not sound for $\langle\alpha\rangle$.

### 5.2 Example Proofs

This section illustrates how the uniform substitution calculus for dL can be used to realize a number of different reasoning techniques from the same proof primitives. While the same flexibility enables these different techniques also for proofs of hybrid systems, the following examples focus on differential equations to additionally illustrate how the differential equation axioms in Fig. 3 are meant to be combined.

*Example 30 (Contextual equivalence proof)* The following proof proves a property of a differential equation using differential invariants without having to solve that differential equation. One use of rule US is shown explicitly, other uses of US are similar to obtain and use the other axiom instances. CE is used together with MP.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{x^3\cdot x+x\cdot x^3\geq 0}\,\mathbb{R}}{[x':=x^3]x'\cdot x+x\cdot x'\geq 0}\,[:=]}{[x'=x^3][x':=x^3]x'\cdot x+x\cdot x'\geq 0}\,G \qquad \dfrac{\dfrac{\dfrac{*}{(f(\tilde{x})\cdot g(\tilde{x}))'=(f(\tilde{x}))'\cdot g(\tilde{x})+f(\tilde{x})\cdot(g(\tilde{x}))'}\,{}'}{(x\cdot x)'=(x)'\cdot x+x\cdot(x)'}\,US}{(x\cdot x)'=x'\cdot x+x\cdot x'}\,x'}{(x\cdot x)'\geq 0\leftrightarrow x'\cdot x+x\cdot x'\geq 0}\,CQ}{(x\cdot x\geq 1)'\leftrightarrow x'\cdot x+x\cdot x'\geq 0}\,c'}{[x'=x^3][x':=x^3](x\cdot x\geq 1)'}\,CE}{[x'=x^3](x\cdot x\geq 1)'}\,DE}{x\cdot x\geq 1\rightarrow[x'=x^3]x\cdot x\geq 1}\,DI$$

Previous calculi [13,15] collapse this proof into a single proof step with complicated built-in operator implementations that silently perform the same reasoning in a non-transparent way. The approach presented here combines separate axioms to achieve the same effect in a modular way, with axioms of individual responsibilities internalizing separate logical reasoning principles in *differential-form* dL. Tactics combining the axioms as indicated make the axiomatic way equally convenient. Clever proof structuring, cuts or MP uses enable proofs in which the main argument remains as fast [13,15] while the additional premises subsequently check soundness. Inferences in context such as those portrayed in CE, CQ are impossible in sequent calculus [12].

*Example 31 (Flat proof)* Rules CQ, CE simplify the proof in Example 30 substantially but are not needed because a proof without contextual equivalence is possible:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\ldots\rightarrow((x\cdot x)'\geq 0\leftrightarrow x'\cdot x+x\cdot x'\geq 0)}\,MP \qquad \dfrac{\dfrac{\dfrac{*}{(f(\tilde{x})\cdot g(\tilde{x}))'=(f(\tilde{x}))'\cdot g(\tilde{x})+f(\tilde{x})\cdot(g(\tilde{x}))'}\,{}'}{(x\cdot x)'=(x)'\cdot x+x\cdot(x)'}\,US}{(x\cdot x)'=x'\cdot x+x\cdot x'}\,x'}{(x\cdot x)'\geq 0\leftrightarrow x'\cdot x+x\cdot x'\geq 0}\,G}{[x':=x^3]((x\cdot x)'\geq 0\leftrightarrow x'\cdot x+x\cdot x'\geq 0)}\,K,K}{[x':=x^3](x\cdot x)'\geq 0\leftrightarrow[x':=x^3]x'\cdot x+x\cdot x'\geq 0}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{see above}}{[x':=x^3](x\cdot x)'\geq 0}\,\text{MP}}{[x'=x^3][x':=x^3](x\cdot x)'\geq 0}\,\text{G}}{[x'=x^3](x\cdot x)'\geq 0}\,\text{DE}}{x\cdot x\geq 1\to[x'=x^3]x\cdot x\geq 1}\,\text{DI}\qquad \dfrac{\dfrac{*}{x^3\cdot x+x\cdot x^3\geq 0}\,\mathbb{R}}{[x':=x^3]x'\cdot x+x\cdot x'\geq 0}\,[:=]$$

*Example 32 (Parametric proof)* The proofs in Examples 30 and 31 use (implicit) cuts with equivalences that predict the outcome of the right premise, which is conceptually simple but inconvenient for proof search. More constructively, a direct proof can use a free function symbol $j(x,x')$ to obtain a straightforward parametric proof, instead:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{j(x,x^3)\geq 0}{[x':=x^3]j(x,x')\geq 0}\,[:=]}{[x'=x^3][x':=x^3]j(x,x')\geq 0}\,\text{G}\qquad \dfrac{\dfrac{(x\cdot x)'=j(x,x')}{(x\cdot x)'\geq 0\leftrightarrow j(x,x')\geq 0}\,\text{CQ}}{(x\cdot x\geq 1)'\leftrightarrow j(x,x')\geq 0}}{[x'=x^3][x':=x^3](x\cdot x\geq 1)'}\,\text{CE}}{[x'=x^3](x\cdot x\geq 1)'}\,\text{DE}}{x\cdot x\geq 1\to[x'=x^3]x\cdot x\geq 1}\,\text{DI}$$

After conducting this proof with two open premises, the free function symbol $j(x,x')$ can be instantiated as needed by a uniform substitution (USR from Theorem 27). The above proof justifies the locally sound inference on the left whose two open premises and conclusions are instantiated by USR leading to the new sound proof on the right:

$$\dfrac{j(x,x^3)\geq 0\qquad (x\cdot x)'=j(x,x')}{x\cdot x\geq 1\to[x'=x^3]x\cdot x\geq 1}\quad\text{implies}\ \text{USR}\ \dfrac{x^3\cdot x+x\cdot x^3\geq 0\qquad (x\cdot x)'=x'\cdot x+x\cdot x'}{x\cdot x\geq 1\to[x'=x^3]x\cdot x\geq 1}$$

After the instantiation of $j(x,x')$ by USR, the right proof completes as follows:

$$\dfrac{\dfrac{\dfrac{*}{x^3\cdot x+x\cdot x^3\geq 0}\,\mathbb{R}\qquad \dfrac{\dfrac{*}{(f(\bar{x})\cdot g(\bar{x}))'=(f(\bar{x}))'\cdot g(\bar{x})+f(\bar{x})\cdot(g(\bar{x}))'}\,{}'}{(x\cdot x)'=(x)'\cdot x+x\cdot(x)'}\,\text{US}}{(x\cdot x)'=x'\cdot x+x\cdot x'}\,x'}{x\cdot x\geq 1\to[x'=x^3]x\cdot x\geq 1}\,\text{USR}$$

This technique helps invariant search, where a free predicate symbol $p(\bar{x})$ is instantiated lazily by USR once all conditions become clear. This reduction saves considerable proof effort compared to eager invariant instantiation in sequent calculi [12].

*Example 33 (Forward computation proof)* The proof in Examples 32 involves less search than the proofs of the same formula in Examples 30 and 31. But it still ultimately requires foresight to identify the appropriate instantiation of $j(x,x')$ for which the proof closes. For invariant search, such proof search is essentially unavoidable [14] even if the technique in Example 32 maximally postpones the search.

When used from left to right, the differential axioms $c'$, $x'+'$, $\cdot'$, $\circ'$ compute deterministically and always simplify terms by pushing differential operators inside. For example, all backwards proof search in the right branch of the last proof of Example 32 can be replaced by a deterministic forward computation proof starting from reflexivity $(x\cdot x)'=(x\cdot x)'$ and drawing on axiom instances (used in a term context via CT) as needed in a forward proof, until the desired output shape is identified:

$$\left|\begin{array}{l}\mathbb{R}\;\dfrac{*}{(x\cdot x)' = (x\cdot x)'}\\[2ex] \cdot'\;\dfrac{(x\cdot x)' = (x)'\cdot x + x\cdot (x)'}{}\\[2ex] x'\;(x\cdot x)' = x'\cdot x + x\cdot x'\end{array}\right.$$

Efficient proof search combines this forward computation proof technique with the backward proof search from Example 32 with advantages similar to other combinations of computation and axiomatic reasoning [5]. Even the remaining positions where axioms still match can be precomputed as a simple function of the axiom that has been applied, e.g., from its fixed pattern of occurrences of differential operators.

*Example 34 (Axiomatic differential equation solver)* Axiomatic equivalence proofs for solving differential equations involve DG for introducing a time variable $t$, DC to cut the solutions in, DW to export the solution to the postcondition, inverse DC to remove the evolution domain constraints again, inverse DG (or the universal strengthening of DG with $\forall y$ instead of $\exists y$ from Theorem 38) to remove the original differential equations, and finally DS to solve the differential equation for time:

$$\begin{array}{ll}
 & \dfrac{*}{\phi \rightarrow \forall s{\geq}0\,(x_0 + \frac{a}{2}s^2 + v_0 s \geq 0)}\\[2ex]
\mathbb{R} & \dfrac{\phi \rightarrow \forall s{\geq}0\,(x_0 + \frac{a}{2}s^2 + v_0 s \geq 0)}{\phi \rightarrow \forall s{\geq}0\,[t := 0 + 1s]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}\\[2ex]
[:=] & \dfrac{\phi \rightarrow \forall s{\geq}0\,[t := 0 + 1s]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}{\phi \rightarrow [t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}\\[2ex]
\mathrm{DS} & \dfrac{\phi \rightarrow [t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}{\phi \rightarrow [v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}\\[2ex]
\mathrm{DG} & \dfrac{\phi \rightarrow [v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}{\phi \rightarrow [x' = v, v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}\ \triangleright\\[2ex]
\mathrm{DC} & \dfrac{\phi \rightarrow [x' = v, v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}\ \triangleright\\[2ex]
\mathrm{DC} & \dfrac{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0 t]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0}\\[2ex]
\mathrm{G,K} & \dfrac{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0 t](x = x_0 + \frac{a}{2}t^2 + v_0 t \rightarrow x \geq y)}{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0 t]x \geq y}\\[2ex]
\mathrm{DW} & \dfrac{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0 t]x \geq y}{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at]x \geq y}\ \triangleright\\[2ex]
\mathrm{DC} & \dfrac{\phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at]x \geq y}{\phi \rightarrow [x' = v, v' = a, t' = 1]x \geq y}\ \triangleright\\[2ex]
 & \dfrac{\phi \rightarrow [x' = v, v' = a, t' = 1]x \geq y}{\phi \rightarrow \exists t\,[x' = v, v' = a, t' = 1]x \geq y}\\[2ex]
\mathrm{DG} & \phi \rightarrow [x' = v, v' = a]x \geq y
\end{array}$$

where $\phi$ is $a \geq 0 \wedge v = v_0 \geq 0 \wedge x = x_0 \geq 0$. The existential quantifier for $t$ is instantiated by 0 (suppressed in the proof for readability reasons). The 4 uses of DC lead to 2 additional premises (marked by $\triangleright$) proving that $v = v_0 + at$ and then $x = x_0 + \frac{a}{2}t^2 + v_0 t$ are differential invariants (using DI, DE, DW). Shortcuts using only DW instead are possible. But the elaborate proof above generalizes to $\langle\rangle$ because it is an equivalence proof. The additional premises for DC with $v = v_0 + at$ prove as follows:

$$\begin{array}{ll}
 & \dfrac{*}{(f(\tilde{x}) + g(\tilde{x}))' = (f(\tilde{x}))' + (g(\tilde{x}))'}\\[2ex]
+' & \dfrac{(f(\tilde{x}) + g(\tilde{x}))' = (f(\tilde{x}))' + (g(\tilde{x}))'}{(v_0 + at)' = (v_0)' + (at)'}\\[2ex]
\mathrm{US} & \dfrac{(v_0 + at)' = (v_0)' + (at)'}{(v_0 + at)' = 0 + a(t')}\\[2ex]
\cdot' & \dfrac{(v_0 + at)' = 0 + a(t')}{v' = (v_0 + at)' \leftrightarrow v' = 0 + at'}\\[2ex]
\mathrm{CQ} & \dfrac{v' = (v_0 + at)' \leftrightarrow v' = 0 + at'}{(v = v_0 + at)' \leftrightarrow v' = 0 + at'}\\[2ex]
\mathbb{R} & \dfrac{*}{a = 0 + a\cdot 1}\\[2ex]
[:=] & \dfrac{a = 0 + a\cdot 1}{[v' := a][t' := 1]v' = 0 + at'}\\[2ex]
\mathrm{CE} & \dfrac{[v' := a][t' := 1]v' = 0 + at' \qquad [v' := a][t' := 1](v = v_0 + at)'}{[v' := a][t' := 1](v = v_0 + at)'}\\[2ex]
\mathrm{G} & \dfrac{[v' := a][t' := 1](v = v_0 + at)'}{[x' = v, v' = a, t' = 1][v' := a][t' := 1](v = v_0 + at)'}\\[2ex]
\mathrm{DE} & \dfrac{[x' = v, v' = a, t' = 1][v' := a][t' := 1](v = v_0 + at)'}{[x' = v, v' = a, t' = 1](v = v_0 + at)'}\\[2ex]
\mathrm{DI} & \dfrac{[x' = v, v' = a, t' = 1](v = v_0 + at)'}{\phi \rightarrow [x' = v, v' = a, t' = 1]v = v_0 + at}
\end{array}$$

After that, the additional premises for DC with $x = x_0 + \frac{a}{2}t^2 + v_0 t$ prove as follows:

$$\dfrac{\dfrac{\dfrac{}{v = v_0 + at \to v = at \cdot 1 + v_0 \cdot 1}\,\mathbb{R}}{v = v_0 + at \to [x' := v][t' := 1]x' = att' + v_0 t'}\,[:=] \qquad \dfrac{\dfrac{\dfrac{}{2\frac{a}{2}tt' + v_0 t' = att' + v_0 t'}\,\mathbb{R}}{(x_0 + \frac{a}{2}t^2 + v_0 t)' = att' + v_0 t'}\,{+',\cdot'}}{x' = (x_0 + \frac{a}{2}t^2 + v_0 t)' \leftrightarrow x' = att' + v_0 t'}\,CQ}{(x = x_0 + \frac{a}{2}t^2 + v_0 t)' \leftrightarrow x' = att' + v_0 t'}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{v = v_0 + at \to [x' := v][t' := 1](x = x_0 + \frac{a}{2}t^2 + v_0 t)'}\,CE}{[x' = v, v' = a, t' = 1 \,\&\, v = v_0 + at](v = v_0 + at \to [x' := v][t' := 1](x = x_0 + \frac{a}{2}t^2 + v_0 t)')}\,G}{[x' = v, v' = a, t' = 1 \,\&\, v = v_0 + at][x' := v][t' := 1](x = x_0 + \frac{a}{2}t^2 + v_0 t)'}\,DW}{[x' = v, v' = a, t' = 1 \,\&\, v = v_0 + at](x = x_0 + \frac{a}{2}t^2 + v_0 t)'}\,DE}{\phi \to [x' = v, v' = a, t' = 1 \,\&\, v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t}\,DI$$

This axiomatic differential equation solving technique is not limited to differential equation systems that can be solved in full, but also works when only part of the differential equations have definable solutions. Contrast this constructive formal proof with the unverified use of a differential equation solver in axiom schema [′] from p. 2.

### 5.3 Differential Substitution Lemmas

In similar ways how the uniform substitution lemmas are the key ingredients that relate syntactic and semantic substitution for the soundness of proof rule US, this section proves the key ingredients relating syntax and semantics of differentials that will be used for the soundness proofs of the differential axioms. Differentials $(\eta)'$ have a local semantics in isolated states, which is crucial for well-definedness. The DI axiom relates truth along a differential equation to initial truth with truth of differentials along a differential equation. The key insight for its soundness is that the analytic time-derivative of the value of a term $\eta$ along any differential equation $x' = \theta \,\&\, \psi$ agrees with the values of its differential $(\eta)'$ along that differential equation. Recall from Definition 7 that $I, \varphi \models x' = \theta \wedge \psi$ indicates that the function $\varphi$ solves the differential equation $x' = \theta \,\&\, \psi$ in interpretation $I$, of which the only important part for the next lemma is that it gives $x'$ the value of the time-derivative of $x$ along the solution $\varphi$.

**Lemma 35** (Differential) *If $I, \varphi \models x' = \theta \wedge \psi$ holds for some solution $\varphi : [0, r] \to \mathcal{S}$ of any duration $r > 0$, then for all times $0 \leq \zeta \leq r$ and all terms $\eta$ with $\mathsf{FV}(\eta) \subseteq \{x\}$:*

$$I\varphi(\zeta)[\![(\eta)']\!] = \frac{\mathsf{d}I\varphi(t)[\![\eta]\!]}{\mathsf{d}t}(\zeta)$$

The differential effect axiom DE axiomatizes the effect of differential equations on the differential symbols. The key insight for its soundness is that differential symbol $x'$ already has the value $\theta$ along the differential equation $x' = \theta$ such that the subsequent differential assignment $x' := \theta$ that assigns the value of $\theta$ to $x'$ has no effect on the truth of the postcondition. The differential substitution resulting from a subsequent use of axiom [:=] is crucial to relay the values of the time-derivatives of the state variables $x$ along a differential equation by way of their corresponding differential symbol $x'$, though. In combination, this makes it possible to soundly substitute the right-hand side of a differential equation for its left-hand side in a proof.

**Lemma 36** (Differential assignment) *If $I, \varphi \models x' = \theta \wedge \psi$ where $\varphi : [0, r] \to \mathcal{S}$ is a solution of any duration $r \geq 0$, then*

$$I, \varphi \models \phi \leftrightarrow [x' := \theta]\phi$$

The final insights for differential invariant reasoning for differential equations are syntactic ways of computing differentials, which can be internalized as axioms ($c'$, $x'+'$, $\cdot'$, $\circ'$), since differentials are represented syntactically in differential-form dL. It is the local semantics as differential forms that makes it possible to soundly capture the interaction of differentials with arithmetic operators by local equations.

**Lemma 37** (Derivations) *The following equations of differentials are valid:*

$$(f)' = 0 \qquad \text{for arity 0 functions or numbers } f \tag{3}$$

$$(x)' = x' \qquad \text{for variables } x \in \mathcal{V} \tag{4}$$

$$(\theta+\eta)' = (\theta)' + (\eta)' \tag{5}$$

$$(\theta\cdot\eta)' = (\theta)'\cdot\eta + \theta\cdot(\eta)' \tag{6}$$

$$[y:=\theta][y':=1]\big((f(\theta))' = (f(y))'\cdot(\theta)'\big) \qquad \text{for } y, y' \notin \mathsf{FV}(\theta) \tag{7}$$

### 5.4 Soundness

The uniform substitution calculus for differential-form dL is *sound*, i.e. all formulas that it proves from valid premises are valid. The soundness argument is entirely modular. The concrete dL axioms in Figs. 2 and 3 are valid formulas and the axiomatic proof rules (i.e. pairs of formulas) in Fig. 2 are locally sound, which implies soundness. The uniform substitution rule is sound so only concludes valid formulas from valid premises (Theorem 26), which implies that dL axioms (and other provable dL formulas) can only be instantiated soundly by rule US. Uniform substitution instances of locally sound axiomatic proof rules (and other locally sound inferences) are locally sound (Theorem 27), which implies that dL axiomatic proof rules in Fig. 2 can only be instantiated soundly by uniform substitutions (USR).

The soundness proof follows a high-level strategy that is similar to earlier proofs [13–15], but ends up in stronger results since all axioms for differential equations are equivalences now. The availability of differentials and differential assignments as syntactic elements in differential-form dL as well as the instantiation support from uniform substitutions makes those soundness proofs significantly more modular, too. For example, what used to be a single proof rule for differential invariants [13] can now be decomposed into separate modular axioms.

**Theorem 38** (Soundness) *The uniform substitution calculus for* dL *is* sound*, that is, every formula that is provable by the* dL *axioms and proof rules is valid, i.e. true in all states of all interpretations. The axioms in Figs. 2 and 3 are valid formulas and the axiomatic proof rules in Fig. 2 are locally sound.*

*Proof* The axioms (and most proof rules) in Fig. 2 are special instances of corresponding axiom schemata and proof rules for differential dynamic logic [14] and, thus, sound.[4] All proof rules in Fig. 2 (but not US itself) are even locally sound, which implies soundness, i.e. that their conclusions are valid (in all $I$) if their premises are. In preparation for a completeness argument, note that rules $\forall$, MP can be augmented soundly to use $p(\bar{x})$ instead of $p(x)$ or $p$, respectively, such that the $\mathsf{FV}(\sigma)=\emptyset$ requirement of Theorem 27 will be met during USR instances of all axiomatic proof rules. The axioms in Fig. 3 are new and need new soundness arguments.

[4] The uniform substitution proof calculus improves modularity and gives stronger equivalence formulations of axioms, though.

DW Soundness of DW uses that differential equations never leave their evolution domain by Definition 7. To show $\nu \in I[\![[x' = f(x) \,\&\, q(x)]q(x)]\!]$, consider any $\varphi : [0, r] \to \mathscr{S}$ of any duration $r \geq 0$ solving $I, \varphi \models x' = f(x) \wedge q(x)$. Then $I, \varphi \models q(x)$ especially $\varphi(r) \in I[\![q(x)]\!]$.

DC Soundness of DC is a stronger version of soundness for the differential cut rule [13]. DC is a differential version of the modal modus ponens K. Only the direction "$\leftarrow$" of the equivalence in DC needs the outer assumption $[x' = f(x) \,\&\, q(x)]r(x)$, but the proof of the conditional equivalence in DC is simpler:

$$[x' = f(x) \,\&\, q(x)]r(x) \to \big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \wedge r(x)]p(x)\big)$$

The core is that if $[x' = f(x) \,\&\, q(x)]r(x)$, so $r(x)$ holds after that differential equation, and if $p(x)$ holds after the differential equation $x' = f(x) \,\&\, q(x) \wedge r(x)$ that is additionally restricted to $r(x)$, then $p(x)$ holds after the differential equation $x' = f(x) \,\&\, q(x)$ with no additional restriction. Let $\nu \in I[\![[x' = f(x) \,\&\, q(x)]r(x)]\!]$. Since all restrictions of solutions are solutions, this is equivalent to $I, \varphi \models r(x)$ for all $\varphi$ of any duration solving $I, \varphi \models x' = f(x) \wedge q(x)$ and starting in $\varphi(0) = \nu$ on $\{x'\}^{\complement}$. So, for all $\varphi$ starting in $\varphi(0) = \nu$ on $\{x'\}^{\complement}$: $I, \varphi \models x' = f(x) \wedge q(x)$ is equivalent to $I, \varphi \models x' = f(x) \wedge q(x) \wedge r(x)$. Hence, $\nu \in I[\![[x' = f(x) \,\&\, q(x) \wedge r(x)]p(x)]\!]$ is equivalent to $\nu \in I[\![[x' = f(x) \,\&\, q(x)]p(x)]\!]$.

DE Axiom DE is new to differential-form $\mathsf{dL}$. Its soundness proof exploits Lemma 36. Consider any state $\nu$. Then $\nu \in I[\![[x' = f(x) \,\&\, q(x)]p(x, x')]\!]$ iff $\varphi(r) \in I[\![p(x, x')]\!]$ for all solutions $\varphi : [0, r] \to \mathscr{S}$ of $I, \varphi \models x' = f(x) \wedge q(x)$ of any duration $r$ starting in $\varphi(0) = \nu$ on $\{x'\}^{\complement}$. That is equivalent to: for all $\varphi$, if $I, \varphi \models x' = f(x) \wedge q(x)$ then $I, \varphi \models p(x, x')$. By Lemma 36, $I, \varphi \models p(x, x')$ iff $I, \varphi \models [x' := f(x)]p(x, x')$, so that is equivalent to $\varphi(r) \in I[\![[x' := f(x)]p(x, x')]\!]$ for all solutions $\varphi : [0, r] \to \mathscr{S}$ of $I, \varphi \models x' = f(x) \wedge q(x)$ of any duration $r$ starting in $\varphi(0) = \nu$ on $\{x'\}^{\complement}$, which is, consequently, equivalent to $\nu \in I[\![[x' = f(x) \,\&\, q(x)][x' := f(x)]p(x, x')]\!]$.

DI Soundness of DI has some relation to the soundness proof for differential invariants [13], yet proves an equivalence and is generalized to leverage differentials. If $\nu \in I[\![[x' = f(x) \,\&\, q(x)]p(x)]\!]$ then the solution $\varphi$ of duration 0 implies that $\nu \in I[\![p(x)]\!]$ since $x' \notin \mathrm{FV}(p(x))$ by Lemma 11, provided that $\varphi(0) \in I[\![q(x)]\!]$, i.e. $\nu \in I[\![q(x)]\!]$ since $x' \notin \mathrm{FV}(q(x))$, such that there is a solution at all. Thus, $[x' = f(x) \,\&\, q(x)]p(x) \to [?q(x)]p(x)$ is valid even without the assumption. Converse $\big(q(x) \to [x' = f(x) \,\&\, q(x)](p(x))'\big) \to [?q(x)]p(x) \to [x' = f(x) \,\&\, q(x)]p(x)$ is only shown for $p(x) \overset{\text{def}}{\equiv} g(x) \geq 0$, where $(p(x))' \equiv ((g(x))' \geq 0)$, because the variations for other formulas are the same as the variations in previous work [13]. Consider a state $\nu$ in which $\nu \in I[\![q(x) \to [x' = f(x) \,\&\, q(x)](p(x))']\!]$. If $\nu \notin I[\![q(x)]\!]$, there is nothing to show, because there is no solution of $x' = f(x) \,\&\, q(x)$ for any duration since $x' \notin \mathrm{FV}(q(x))$, so $\nu \in I[\![[x' = f(x) \,\&\, q(x)]p(x)]\!]$ holds vacuously. Otherwise, $\nu \in I[\![q(x)]\!]$, which implies $\nu \in I[\![[x' = f(x) \,\&\, q(x)](p(x))']\!]$ by assumption. Assume $\nu \in I[\![[?q(x)]p(x)]\!]$, so $\nu \in I[\![p(x)]\!]$ since $\nu \in I[\![q(x)]\!]$. To show that $\nu \in I[\![[x' = f(x) \,\&\, q(x)]p(x)]\!]$ consider any solution $\varphi$ of any duration $r \geq 0$. The case $r = 0$ follows from $\nu \in I[\![p(x)]\!]$ by Lemma 11 since $\mathrm{FV}(p(x)) = \{x\}$ is disjoint from $\{x'\}$, which, unlike $x$, is changed by evolutions of any duration, including 0. That leaves the case $r > 0$.

Let $\varphi$ be a solution of $x' = f(x) \,\&\, q(x)$ according to Definition 7, so $\nu = \varphi(0)$ on $\{x'\}^{\complement}$ and $I, \varphi \models x' = f(x) \,\&\, q(x)$. Now $\nu \in I[\![[x' = f(x) \,\&\, q(x)](p(x))']\!]$ implies $I, \varphi \models (p(x))'$. As $r > 0$, Lemma 35 implies $0 \leq I\varphi(\zeta)[\![(g(x))']\!] = \frac{\mathrm{d} I\varphi(t)[\![g(x)]\!]}{\mathrm{d}t}(\zeta)$

for all $\zeta$ since $\mathrm{FV}(g(x)) = \{x\}$. Together with $\varphi(0) \in I[\![p(x)]\!]$ (by Lemma 11 and $\mathrm{FV}(p(x)) \cap \{x'\} = \emptyset$ from $\nu \in I[\![p(x)]\!]$), which is $\varphi(0) \in I[\![g(x) \geq 0]\!]$, this implies $\varphi(\zeta) \in I[\![g(x) \geq 0]\!]$ for all $\zeta$, including $r$, by the mean-value theorem, since $I\varphi(r)[\![g(x)]\!] - I\varphi(0)[\![g(x)]\!] = (r-0)\frac{\mathrm{d}I\varphi(t)[\![g(x)]\!]}{\mathrm{d}t}(\zeta) \geq 0$ for some $\zeta \in (0,r)$. The mean-value theorem (Lemma 41 in "Appendix") is applicable since the value $I\varphi(t)[\![g(x)]\!]$ of term $g(x)$ along $\varphi$ is continuous in $t$ on $[0,r]$ and differentiable on $(0,r)$ as compositions of the, by Definition 5 smooth, evaluation function and the differentiable solution $\varphi(t)$ of a differential equation.

DG Soundness of DG is a constructive variation of the soundness proof for differential auxiliaries [15]. Let $\nu \in I[\![\exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)]\!]$, that is, $\nu^d_y \in I[\![[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)]\!]$ for some value $d \in \mathbb{R}$. In order to show that $\nu \in I[\![[x' = f(x)\,\&\,q(x)]p(x)]\!]$, consider any $\varphi : [0,r] \to \mathscr{S}$ such that $I, \varphi \models x' = f(x) \wedge q(x)$ and $\varphi(0) = \nu$ on $\{x'\}^{\complement}$. By modifying the values of $y, y'$ along $\varphi$, this function can be augmented to a solution $\tilde{\varphi} : [0,r] \to \mathscr{S}$ such that $I, \tilde{\varphi} \models x' = f(x) \wedge y' = a(x)y + b(x) \wedge q(x)$ and $\tilde{\varphi}(0)(y) = d$ as shown below. The assumption then implies $\tilde{\varphi}(r) \in I[\![p(x)]\!]$, which, by Lemma 11, is equivalent to $\varphi(r) \in I[\![p(x)]\!]$ since $y, y' \notin \mathrm{FV}(p(x))$ and $\varphi(r) = \tilde{\varphi}(r)$ on $\{y, y'\}^{\complement}$, which implies $\nu \in I[\![[x' = f(x)\,\&\,q(x)]p(x)]\!]$, since $\varphi$ was arbitrary.

The construction of the modification $\tilde{\varphi}$ of $\varphi$ on $\{y, y'\}$ proceeds as follows. By Picard-Lindelöf's theorem (Theorem 43 in the "Appendix"), there is a unique solution $y : [0,r] \to \mathbb{R}$ of the initial-value problem

$$\begin{aligned} y(0) &= d \\ y'(t) = F(t, y(t)) &\overset{\text{def}}{=} y(t)(I\varphi(t)[\![a(x)]\!]) + I\varphi(t)[\![b(x)]\!] \end{aligned} \tag{8}$$

because $F(t,y)$ is continuous on $[0,r] \times \mathbb{R}$ (since $I\varphi(t)[\![a(x)]\!]$ and $I\varphi(t)[\![b(x)]\!]$ are continuous in $t$ as compositions of the, by Definition 5 smooth, evaluation function and the continuous solution $\varphi(t)$ of a differential equation) and because $F(t,y)$ satisfies the Lipschitz condition

$$\|F(t,y) - F(t,z)\| = \|(y-z)(I\varphi(t)[\![a(x)]\!])\| \leq \|y - z\| \max_{t \in [0,r]} I\varphi(t)[\![a(x)]\!]$$

where the maximum exists, because it is a maximum of a continuous function on the compact set $[0,r]$. The modification $\tilde{\varphi}$ agrees with $\varphi$ on $\{y, y'\}^{\complement}$. On $\{y, y'\}$, the modification $\tilde{\varphi}$ is defined as $\tilde{\varphi}(t)(y) = y(t)$ and $\tilde{\varphi}(t)(y') = F(t, y(t))$, respectively, for the solution $y(t)$ of (8). In particular $\tilde{\varphi}(t)(y')$ agrees with the time-derivative $y'(t)$ of the value $\tilde{\varphi}(t)(y) = y(t)$ of $y$ along $\tilde{\varphi}$. By construction, $\tilde{\varphi}(0)(y) = d$ and $I, \tilde{\varphi} \models x' = f(x) \wedge y' = a(x)y + b(x) \wedge q(x)$, because $y' = a(x)y + b(x)$ holds along $\tilde{\varphi}$ by (8) and because $\varphi(t) = \tilde{\varphi}(t)$ on $\{y, y'\}^{\complement}$ so that $x' = f(x) \wedge q(x)$ continues to hold along $\tilde{\varphi}$ by Lemma 10 because $y, y' \notin \mathrm{FV}(x' = f(x) \wedge q(x))$.

Conversely, let $\nu \in I[\![[x' = f(x)\,\&\,q(x)]p(x)]\!]$. This direction shows a stronger version of $\nu \in I[\![\exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)]\!]$ by showing for all terms $\eta$ that $\nu \in I[\![\forall y\,[x' = f(x), y' = \eta\,\&\,q(x)]p(x)]\!]$. Consider any $d \in \mathbb{R}$ and term $\eta$ and show $\nu^d_y \in I[\![[x' = f(x), y' = \eta\,\&\,q(x)]p(x)]\!]$. Consider any $\varphi : [0,r] \to \mathscr{S}$ such that $I, \varphi \models x' = f(x) \wedge y' = \eta \wedge q(x)$ with $\varphi(0) = \nu^d_y$ on $\{x', y'\}^{\complement}$. Then the restriction $\varphi|_{\{y,y'\}^{\complement}}$ of $\varphi$ to $\{y, y'\}^{\complement}$ with $\varphi|_{\{y,y'\}^{\complement}}(t) = \nu^d_y$ on $\{y, y'\}$ for all $t \in [0,r]$ still solves $I, \varphi|_{\{y,y'\}^{\complement}} \models x' = f(x) \wedge q(x)$ by Lemma 10 since $\varphi|_{\{y,y'\}^{\complement}} = \varphi$ on $\{y, y'\}^{\complement}$ and $y, y' \notin \mathrm{FV}(x' = f(x) \wedge q(x))$. It also satisfies $\varphi|_{\{y,y'\}^{\complement}}(0) = \nu^d_y$ on $\{x'\}^{\complement}$,

because $\varphi(0) = \nu_y^d$ on $\{x', y'\}^{\complement}$ yet $\varphi|_{\{y,y'\}^{\complement}}(t)(y') = \nu_y^d(y')$. Thus, by assumption, $\varphi|_{\{y,y'\}^{\complement}}(r) \in I[\![p(x)]\!]$, which implies $\varphi(r) \in I[\![p(x)]\!]$ by Lemma 11, because $\varphi = \varphi|_{\{y,y'\}^{\complement}}$ on $\{y, y'\}^{\complement}$ and $y, y' \notin \mathrm{FV}(p(x))$.

In particular, axiom DG continues to be sound when replacing $\exists y$ by $\forall y$.

DS Soundness of the solution axiom DS follows from existence and uniqueness of global solutions of constant differential equations. Consider any state $\nu$. By Theorem 43, there is a unique global solution $\varphi : [0, \infty) \to \mathscr{S}$ defined as $\varphi(\zeta)(x) \overset{\text{def}}{=} I\nu_t^{\zeta}[\![x + ft]\!]$ and $\varphi(\zeta)(x') \overset{\text{def}}{=} \frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(\zeta) = I(f)$ and $\varphi(\zeta) = \nu$ on $\{x, x'\}^{\complement}$. This solution satisfies $\varphi(0) = \nu(x)$ on $\{x'\}^{\complement}$ and $I, \varphi \models x' = f$, i.e. $\varphi(\zeta) \in I[\![x' = f]\!]$ for all $0 \leq \zeta \leq r$. All solutions of $x' = f$ from initial state $\nu$ are restrictions of $\varphi$ to subintervals of $[0, \infty)$. The (unique) state $\omega$ that satisfies $(\nu_t^{\zeta}, \omega) \in I[\![x := x + ft]\!]$ satisfies the agreement $\omega = \varphi(\zeta)$ on $\{x'\}^{\complement}$, so that, by $x' \notin \mathrm{FV}(p(x))$, Lemma 11 implies that $\omega \in I[\![p(x)]\!]$ iff $\varphi(\zeta) \in I[\![p(x)]\!]$.

First consider axiom $[x' = f]p(x) \leftrightarrow \forall t{\geq}0\, [x := x + ft]p(x)$ for the special case $q(x) \equiv \mathit{true}$. If $\nu \in I[\![[x' = f]p(x)]\!]$, then $\varphi(\zeta) \in I[\![p(x)]\!]$ for all $\zeta \geq 0$, because the restriction of $\varphi$ to $[0, \zeta]$ solves $x' = f$ from $\nu$, thus $\omega \in I[\![p(x)]\!]$ since $\omega = \varphi(\zeta)$ on $\{x'\}^{\complement}$ and $x' \notin \mathrm{FV}(p(x))$ by Lemma 11, which implies $\nu_t^{\zeta} \in I[\![[x := x + ft]p(x)]\!]$, so $\nu \in I[\![\forall t{\geq}0\, [x := x + ft]p(x)]\!]$ as $\zeta \geq 0$ was arbitrary.

Conversely, $\nu \in I[\![\forall t{\geq}0\, [x := x + ft]p(x)]\!]$ implies $\nu_t^{\zeta} \in I[\![[x := x + ft]p(x)]\!]$ for all $\zeta \geq 0$, i.e. $\omega \in I[\![p(x)]\!]$ when $(\nu_t^{\zeta}, \omega) \in I[\![x := x + ft]\!]$. Lemma 11 again implies $\varphi(\zeta) \in I[\![p(x)]\!]$ for all $\zeta \geq 0$ since $x' \notin \mathrm{FV}(p(x))$, so $\nu \in I[\![[x' = f]p(x)]\!]$, since all solutions are restrictions of $\varphi$.

Soundness of DS follows using that all solutions $\varphi : [0, r] \to \mathscr{S}$ of $x' = f(x)\,\&\,q(x)$ satisfy $\varphi(\zeta) \in I[\![q(x)]\!]$ for all $0 \leq \zeta \leq r$, which, using Lemma 11 as above, is equivalent to $\nu \in I[\![\forall 0{\leq}s{\leq}t\, q(x + fs)]\!]$ when $\nu(t) = r$.

$+', \cdot', \circ', x'$ Soundness of the derivation axioms $+', \cdot', \circ'$ as well as $c', x'$ follows from Lemma 37, since they are special instances of (5), (6) and (7) as well as (3) and (4), respectively. For axiom $\circ'$ observe that $y, y' \notin \mathrm{FV}(g(x))$.

G Let the premise $p(\bar{x})$ be valid in some $I$, i.e. $I \models p(\bar{x})$, i.e. $\omega \in I[\![p(\bar{x})]\!]$ for all $\omega$. Then, the conclusion $[a]p(\bar{x})$ is valid in the same $I$, i.e. $\nu \in I[\![[a]p(\bar{x})]\!]$ for all $\nu$, because $\omega \in I[\![p(\bar{x})]\!]$ for all $\omega$, so also for all $\omega$ with $(\nu, \omega) \in I[\![a]\!]$. Thus, G is locally sound.

∀ Let the premise $p(x)$ be valid in some $I$, i.e. $I \models p(x)$, i.e. $\omega \in I[\![p(x)]\!]$ for all $\omega$. Then, the conclusion $\forall x\, p(x)$ is valid in the same $I$, i.e. $\nu \in I[\![\forall x\, p(x)]\!]$ for all $\nu$, i.e. $\nu_x^d \in I[\![p(x)]\!]$ for all $d \in \mathbb{R}$, because $\omega \in I[\![p(x)]\!]$ for all $\omega$, so in particular for all $\omega = \nu_x^d$ for any real $d \in \mathbb{R}$. Thus, ∀ is locally sound.

CQ Let the premise $f(\bar{x}) = g(\bar{x})$ be valid in some $I$, i.e. $I \models f(\bar{x}) = g(\bar{x})$, which is $\nu \in I[\![f(\bar{x}) = g(\bar{x})]\!]$ for all $\nu$, i.e. $I\nu[\![f(\bar{x})]\!] = I\nu[\![g(\bar{x})]\!]$ for all $\nu$.

Consequently, $I\nu[\![f(\bar{x})]\!] \in I(p)$ iff $I\nu[\![g(\bar{x})]\!] \in I(p)$. So, $I \models p(f(\bar{x})) \leftrightarrow p(g(\bar{x}))$. Thus, CQ is locally sound.

CE Let the premise $p(\bar{x}) \leftrightarrow q(\bar{x})$ be valid in some $I$, i.e. $I \models p(\bar{x}) \leftrightarrow q(\bar{x})$, which is $\nu \in I[\![p(\bar{x}) \leftrightarrow q(\bar{x})]\!]$ for all $\nu$. Consequently, $I[\![p(\bar{x})]\!] = I[\![q(\bar{x})]\!]$. Thus, $I[\![C(p(\bar{x}))]\!] = I(C)\big(I[\![p(\bar{x})]\!]\big) = I(C)\big(I[\![q(\bar{x})]\!]\big) = I[\![C(q(\bar{x}))]\!]$. This implies $I \models C(p(\bar{x})) \leftrightarrow C(q(\bar{x}))$, hence the conclusion is valid in $I$. Thus, CE is locally sound.

MP Modus ponens MP is locally sound with respect to interpretation $I$ *and* state $\nu$, which implies local soundness. If $\nu \in I[\![p \to q]\!]$ and $\nu \in I[\![p]\!]$ then $\nu \in I[\![q]\!]$.

US Rule USR preserves local soundness by Theorem 27 and rule US is sound by Theorem 26, just not locally sound. □

Observe that uniform substitutions are not limited to merely instantiating dL axioms and axiomatic proof rules. Rule US can be used to instantiate any dL formula soundly (Theorem 26), which, in particular, gives a simple mechanism for derived axioms and lemmas, which are just dL formulas that have a proof. Uniform substitutions can instantiate any locally sound proof as well (Theorem 27), which, in particular, gives a simple mechanism for derived axiomatic rules, definitions, and invariant search with lazy instantiation of invariants. These are just proofs from the dL rules and axioms in Figs. 2 and 3 whose premises and conclusions are uniformly substituted to instantiate the requisite function or predicate symbols (recall Example 32).

### 5.5 Completeness

By Theorem 38, the dL calculus is *sound*, so every dL formula that is provable using the dL axioms and proof rules is valid, i.e. true in all states of all interpretations. The more intriguing converse whether the dL calculus is *complete*, i.e. can prove all dL formulas that are valid, has an answer, too. Previous calculi for dL were proved to be complete relative to differential equations [12,14] and also proved complete relative to discrete dynamics [14]. A generalization of the Hilbert calculus to hybrid games was even proved complete schematically [16]. The uniform substitution calculus for differential-form dL is, to a large extent, a specialization of previous calculi tailored to significantly simplify soundness arguments. Yet, completeness does not transfer when restricting proof calculi. In fact, one key question is whether the restrictions imposed upon proofs for soundness purposes by the simple technique of uniform substitutions does also preserve completeness. Indeed, completeness can be shown to carry over from a previous schematic completeness proof for differential game logic [16] using expressiveness results from previous completeness proofs [12,14] by augmenting the schematic completeness proof with instantiability proofs.

The first challenge is to prove that uniform substitutions are flexible enough to prove all required instances of the dL axioms and axiomatic proof rules. For simplicity, consider $p(\bar{x})$ to be a quantifier symbol of arity 0. A dL formula $\varphi$ is called *surjective* iff rule US can instantiate $\varphi$ to any of its axiom schema instances, which are those formulas that are obtained by uniformly replacing program constants $a$ by any hybrid programs and quantifier symbols $C()$ by formulas. An axiomatic rule is called *surjective* iff USR can instantiate it to any of its proof rule schema instances.

**Lemma 39** (Surjective axioms) *If $\varphi$ is a* dL *formula that is built only from quantifier symbols of arity 0 and program constants but no function or predicate symbols, then $\varphi$ is surjective. Axiomatic rules consisting of surjective* dL *formulas are surjective.*

Lemma 39 generalizes to quantifier symbols with arguments that have no function or predicate symbols, since those are always $\mathscr{V}$-admissible. Generalizations to function and predicate symbol instances are possible with adequate care. The axiom [?] is surjective, because it does not have any bound variables, so admissibility of its instances is obvious. Similarly rules MP and, with the twist from the proof of Theorem 38, rule $\forall$ become surjective. Axioms $\forall$i, $\forall\rightarrow$, $\mathrm{V}_\forall$ can be augmented for surjectivity in similar ways, where $\mathrm{V}_\forall$ is surjective when $p$ is instantiated such that $x$ does not occur free, which is a soundness-critical restriction, and $\forall$i is instantiated respecting its shape.

A previous schematic completeness result [16] shows completeness relative to any differentially expressive[5] logic. Lemma 39 makes it easy to augment this proof to show that the schema instantiations required for completeness are provable by US, USR from axioms or axiomatic rules. Both the first-order logic of differential equations [12] and discrete dynamic logic [14] are differentially expressive for dL.

**Theorem 40** (Relative completeness) *The* dL *calculus is a* sound and complete axiomatization *of hybrid systems relative to* any *differentially expressive logic L, i.e. every valid* dL *formula is provable in the* dL *calculus from L tautologies.*

With the expected exceptions of loops and differential equations, the proof of Theorem 40 confirms that successive unification with axiom keys gives a complete proof strategy. The search for applicable positions is deterministic using recursive computations as in Example 33. Loops and differential equations need corresponding (differential) invariant search using parametric predicates $j(x, x')$ as in Example 32.

This result proves that a very simple mechanism, essentially the single proof rule of uniform substitution, makes it possible to prove differential dynamic logic formulas from a parsimonious soundness-critical core with a few concrete formulas as axioms and without losing the completeness that axiom schema calculi enjoy.

## 6 Conclusions

Uniform substitutions lead to a simple and modular proof calculus that is entirely based on axioms and axiomatic rules, instead of soundness-critical schema variables with side-conditions in axiom schemata and proof rules. The US calculus is straightforward to implement, since axioms are just formulas and axiomatic rules are just pairs of formulas and since the uniform substitutions themselves have a straightforward recursive definition. The key ingredient enabling such modularity for differential equations are differential forms that have a local semantics and make it possible to reduce reasoning about *differential equations* to local reasoning about (inequalities or) *equations of differentials*. The increased modularity also enables flexible reasoning by fast contextual equivalence that uniform substitutions provide almost for free.

Overall, uniform substitutions lead to a simple and modular, sound and complete proof calculus for differential dynamic logic that is entirely based on axioms and axiomatic rules. Prover implementations merely reduce to uniform substitutions using the static semantics, starting from one copy of each axiom and axiomatic rule. This leads to significantly simpler and more parsimonious implementations. The soundness-critical core of the uniform substitution prover KeYmaera X [6], for example, is 2.5 % of the size of the core of the sequent calculus prover KeYmaera [19], which, even if implemented in a different programming language, has more complex implementations of proof rules and schema variable matching or built-in operators.

**Acknowledgements** I am grateful to the anonymous reviewers for their helpful feedback. This material is based upon work supported by the National Science Foundation by NSF CAREER Award CNS-1054246.



[5] A logic $L$ closed under first-order connectives is *differentially expressive* (for dL) if every dL formula $\phi$ has an equivalent $\phi^\flat$ in $L$ and all equivalences of the form $\langle x' = \theta \rangle G \leftrightarrow (\langle x' = \theta \rangle G)^\flat$ for $G$ in $L$ are provable in its calculus.

## Appendix: Proofs

This section lists the proofs of the remaining results. The proofs use the following classical results, where $\nabla g$ denotes the gradient of the function $g$ so the vector of all partial derivatives (if it exists).

**Lemma 41** (Mean-value theorem *[22, §10.10])* *If $f : [a,b] \to \mathbb{R}$ is continuous and differentiable in $(a,b)$, then there is a $\xi \in (a,b)$ such that*

$$f(b) - f(a) = f'(\xi)(b-a)$$

**Lemma 42** (Chain rule *[23, §3.10])* *If $f : U \to \mathbb{R}^m$ is differentiable at $t \in U \subseteq \mathbb{R}$ and $g : V \to \mathbb{R}$, with $f(U) \subseteq V \subseteq \mathbb{R}^m$, is differentiable at $f(t) \in V$, then $g \circ f : U \to \mathbb{R}$ is differentiable at $t$ with derivative*

$$(g \circ f)'(t) = (\nabla g)\big(f(t)\big) \cdot f'(t) = \sum_{j=1}^{m} \frac{\partial g}{\partial y_j}\big(f(t)\big) f_j'(t)$$

**Theorem 43** (Global uniqueness theorem of Picard–Lindelöf [24, §10.VII]) *Let $f : [0,a] \times \mathbb{R}^n \to \mathbb{R}^n$ be a continuous function that is Lipschitz continuous with respect to $y$ and let $y_0 \in \mathbb{R}^n$. Then, there is a unique solution of the following initial value problem on $[0,a]$*

$$y'(t) = f(t,y) \qquad y(0) = y_0$$

*Proof of Lemma 9.* First prove that $\mathsf{BV}(\alpha)$ has the bound effect property. Consider any $(\nu,\omega) \in I[\![\alpha]\!]$ and $x \notin \mathsf{BV}(\alpha)$ then $\nu(x) = \omega(x)$ by Definition 8.

Suppose there was a set $V \not\supseteq \mathsf{BV}(\alpha)$ satisfying the bound effect property for $\alpha$. Then there is a variable $x \in \mathsf{BV}(\alpha) \setminus V$, which implies that there are $I$ and there are $(\nu,\omega) \in I[\![\alpha]\!]$ such that $\nu(x) \neq \omega(x)$. But, then $V$ does not have the bound effect property, as $(\nu,\omega) \in I[\![\alpha]\!]$ but it is not the case that $\nu = \omega$ on $V^{\complement}$, since $V^{\complement} \supseteq \{x\}$ yet $\nu(x) \neq \omega(x)$. □

*Proof of Lemma 10.* To prove that $\mathsf{FV}(\theta)$ has the coincidence property, it is enough to show by induction that, for any set of variables $S \subseteq \mathsf{FV}(\theta)^{\complement}$, the state $\nu'$ in between $\nu$ and $\tilde{\nu}$ that is defined as $\nu' = \nu$ on $S$ and as $\nu' = \tilde{\nu}$ on $S^{\complement}$ agrees with $\tilde{\nu}$ in the value $I\nu'[\![\theta]\!] = I\tilde{\nu}[\![\theta]\!]$.

0. For $S = \emptyset$, there is nothing to show as $\nu' = \tilde{\nu}$.
1. For $S \cup \{z\}$ with a variable $z \notin \mathsf{FV}(\theta)$, abbreviate the modified state $\nu'^{\nu(z)}_z$ by $\nu'_z$, which satisfies $\nu'_z = \nu'$ on $\{z\}^{\complement}$, so $I\nu'_z[\![\theta]\!] = I\nu'[\![\theta]\!] = I\tilde{\nu}[\![\theta]\!]$, because $z \notin \mathsf{FV}(\theta)$ and by induction hypothesis.

When $S$ is the set of all variables where $\nu$ and $\tilde{\nu}$ differ, which is $S \subseteq \mathsf{FV}(\theta)^{\complement}$ by assumption, this implies $\nu' = \nu$ so $I\nu[\![\theta]\!] = I\tilde{\nu}[\![\theta]\!]$. Finally, if $I = J$ on $\Sigma(\theta)$ then also $I\tilde{\nu}[\![\theta]\!] = J\tilde{\nu}[\![\theta]\!]$ by an induction.

Suppose there was a set $V \not\supseteq \mathsf{FV}(\theta)$ satisfying the coincidence property for $\theta$. Then there is a variable $x \in \mathsf{FV}(\theta) \setminus V$, which implies that there are $I$, $\nu = \tilde{\nu}$ on $\{x\}^{\complement}$ such that $I\nu[\![\theta]\!] \neq I\tilde{\nu}[\![\theta]\!]$. Then $V$ does not have the coincidence property, as $\nu = \tilde{\nu}$ on $V$ but $I\nu[\![\theta]\!] \neq I\tilde{\nu}[\![\theta]\!]$. □

*Proof of Lemma 11.* To prove that $\mathsf{FV}(\phi)$ has the coincidence property, it is enough to show by induction that, for any set of variables $S \subseteq \mathsf{FV}(\phi)^{\complement}$, the state $\nu'$ in between $\nu$ and $\tilde{\nu}$ that is defined as $\nu' = \nu$ on $S$ and as $\nu' = \tilde{\nu}$ on $S^{\complement}$ agrees with $\tilde{\nu}$ in the truth-value $\nu' \in I[\![\phi]\!]$ iff $\tilde{\nu} \in I[\![\phi]\!]$.

0. For $S = \emptyset$, there is nothing to show as $\nu' = \tilde{\nu}$.
1. For $S \cup \{z\}$ with a variable $z \notin \mathsf{FV}(\phi)$, abbreviate the modified state $\nu'^{\nu(z)}_z$ by $\nu'_z$, which satisfies $\nu'_z = \nu'$ on $\{z\}^{\complement}$, so $\nu'_z \in I[\![\phi]\!]$ iff $\nu' \in I[\![\phi]\!]$, because $z \notin \mathsf{FV}(\phi)$, iff $\tilde{\nu} \in I[\![\phi]\!]$ by induction hypothesis.

When $S$ is the set of all variables where $\nu$ and $\tilde{\nu}$ differ, which is $S \subseteq \mathsf{FV}(\phi)^{\complement}$ by assumption, this implies $\nu' = \nu$ so $\nu \in I[\![\phi]\!]$ iff $\tilde{\nu} \in I[\![\phi]\!]$. Finally, if $I = J$ on $\Sigma(\phi)$ then also $\tilde{\nu} \in I[\![\phi]\!]$ iff $\tilde{\nu} \in J[\![\phi]\!]$ by an induction.

Suppose there was a set $V \not\supseteq \mathsf{FV}(\phi)$ satisfying the coincidence property for $\phi$. Then there is a variable $x \in \mathsf{FV}(\phi) \setminus V$, which implies that there are $I$, $\nu = \tilde{\nu}$ on $\{x\}^{\complement}$ such that $\nu \in I[\![\phi]\!] \not\ni \tilde{\nu}$. Then $V$ does not have the coincidence property, as $\nu = \tilde{\nu}$ on $V$ but $\nu \in I[\![\phi]\!] \not\ni \tilde{\nu}$. □

*Proof of Lemma 12.* To prove that $\mathsf{FV}(\alpha)$ has the coincidence property, it is enough to show by induction for all $S \subseteq \mathsf{FV}(\alpha)^{\complement}$ that the state $\nu'$ in between $\tilde{\nu}$ and $\nu$ that is defined as $\nu' = \tilde{\nu}$ on $S$ and as $\nu' = \nu$ on $S^{\complement}$ has a state $\omega'$ that agrees with $\omega' = \omega$ on $S^{\complement}$ such that $(\nu', \omega') \in I[\![\alpha]\!]$ as well.

0. For $S = \emptyset$, there is nothing to show for $\nu' = \nu$ and $\omega' = \omega$, because $(\nu, \omega) \in I[\![\alpha]\!]$.
1. For $S \cup \{z\}$ with a variable $z \notin \mathsf{FV}(\alpha)$, let $\nu'_z$ denote modified state $\nu'^{\tilde{\nu}(z)}_z$. Then $\nu'_z = \nu'$ on $\{z\}^{\complement}$ and, by induction hypothesis, $(\nu', \omega') \in I[\![\alpha]\!]$ for some $\omega'$ with $\omega' = \omega$ on $S^{\complement}$. Since $z \notin \mathsf{FV}(\alpha)$, this implies there is a state $\omega'_z$ such that $\omega'_z = \omega'$ on $\{z\}^{\complement}$ and $(\nu'_z, \omega'_z) \in I[\![\alpha]\!]$. Thus, $\omega'_z = \omega' = \omega$ on $(S \cup \{z\})^{\complement}$.

Finally the state $\nu'$ resulting for $S = V^{\complement}$ satisfies $\nu' = \tilde{\nu}$ because $\nu' = \tilde{\nu}$ on $V^{\complement}$ and $\nu' = \nu = \tilde{\nu}$ on $(V^{\complement})^{\complement} = V$ already and the state $\tilde{\omega}$ defined as $\omega'$ satisfies $\omega' = \omega$ on $V$ and $(\tilde{\nu}, \tilde{\omega}) \in I[\![\alpha]\!]$. Finally, if $I = J$ on $\Sigma(\alpha)$ then also $(\tilde{\nu}, \tilde{\omega}) \in J[\![\alpha]\!]$.

Suppose there was a set $V \not\supseteq \mathsf{FV}(\alpha)$ satisfying the coincidence property for $\alpha$. Then there is a variable $x \in \mathsf{FV}(\alpha) \setminus V$, which implies that there are $I, \nu, \tilde{\nu}, \omega$ such that $\nu = \tilde{\nu}$ on $\{x\}^{\complement}$ and $(\nu, \omega) \in I[\![\alpha]\!]$, but there is no $\tilde{\omega}$ with $\omega = \tilde{\omega}$ on $\{x\}^{\complement}$ such that $(\tilde{\nu}, \tilde{\omega}) \in I[\![\alpha]\!]$. Then $V$ does not have the coincidence property, because $\nu = \tilde{\nu}$ on $\{x\}^{\complement} \supseteq V$ and $(\nu, \omega) \in I[\![\alpha]\!]$, but there is no $\tilde{\omega}$ with $\omega = \tilde{\omega}$ on $\{x\}^{\complement}$ such that $(\tilde{\nu}, \tilde{\omega}) \in I[\![\alpha]\!]$. □

*Proof of Lemma 17.* First prove $\mathrm{BV}(\alpha) \supseteq \mathsf{BV}(\alpha)$ by a straightforward structural induction on $\alpha$.

1. For program constant $a$, the statement is obvious, since $\mathrm{BV}(a) = \mathscr{V}$.
2. $(\nu, \omega) \in I[\![x := \theta]\!]$ iff $\omega = \nu^r_x$ with $r = I\nu[\![\theta]\!]$ so $\nu = \omega$ except for $\{x\} = \mathrm{BV}(x := \theta) \supseteq \mathsf{BV}(x := \theta)$.
3. $(\nu, \omega) \in I[\![?\psi]\!] = \{(\nu, \nu) : \nu \in I[\![\psi]\!]\}$ implies $\nu = \omega$ so $\mathsf{BV}(?\psi) = \mathrm{BV}(?\psi) = \emptyset$.
4. $(\nu, \omega) \in I[\![x' = \theta \,\&\, \psi]\!]$ implies $\nu = \varphi(0)$ on $\{x'\}^{\complement}$ and $\omega = \varphi(r)$ for some $\varphi$ with $I, \varphi \models x' = \theta \wedge \psi$, so $\varphi(\zeta) = \nu$ on $\{x, x'\}^{\complement}$ for all $\zeta$. Thus $\nu = \omega$ on $\{x, x'\}^{\complement}$ by Definition 7. Hence, $\mathsf{BV}(x' = \theta \,\&\, \psi) \subseteq \{x, x'\} = \mathrm{BV}(x' = \theta \,\&\, \psi)$.
5. $(\nu, \omega) \in I[\![\alpha \cup \beta]\!] = I[\![\alpha]\!] \cup I[\![\beta]\!]$ implies $(\nu, \omega) \in I[\![\alpha]\!]$ or $(\nu, \omega) \in I[\![\beta]\!]$, By induction hypothesis, $\mathsf{BV}(\alpha) \subseteq \mathrm{BV}(\alpha)$ and $\mathsf{BV}(\beta) \subseteq \mathrm{BV}(\beta)$. Either way, $\nu = \omega$ on $(\mathsf{BV}(\alpha) \cup \mathsf{BV}(\beta))^{\complement}$. So, $\mathsf{BV}(\alpha \cup \beta) \subseteq \mathsf{BV}(\alpha) \cup \mathsf{BV}(\beta) \subseteq \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta) = \mathrm{BV}(\alpha \cup \beta)$.

6. $(\nu,\omega) \in I[\![\alpha;\beta]\!] = I[\![\alpha]\!] \circ I[\![\beta]\!]$, i.e. there is a $\mu$ such that $(\nu,\mu) \in I[\![\alpha]\!]$ as well as $(\mu,\omega) \in [\![\beta]\!]$. By induction hypothesis, $\mathsf{BV}(\alpha) \subseteq \mathrm{BV}(\alpha)$ and $\mathsf{BV}(\beta) \subseteq \mathrm{BV}(\beta)$. Thus, $\nu = \mu = \omega$ on $(\mathsf{BV}(\alpha) \cup \mathsf{BV}(\beta))^{\complement}$. So $\mathsf{BV}(\alpha;\beta) \subseteq \mathsf{BV}(\alpha) \cup \mathsf{BV}(\beta) \subseteq \mathrm{BV}(\alpha) \cup \mathrm{BV}(\beta) = \mathrm{BV}(\alpha;\beta)$.
7. The case $(\nu,\omega) \in I[\![\alpha^*]\!] = \bigcup_{n\in\mathbb{N}} I[\![\alpha^n]\!]$ follows by induction on $n$.

The second part proves $\mathrm{FV}(\theta) \supseteq \mathsf{FV}(\theta)$. Let $y \in \mathsf{FV}(\theta)$, which implies that there are $I$ and $\nu = \tilde{\nu}$ on $\{x\}^{\complement}$ such that $I\nu[\![\theta]\!] \neq I\tilde{\nu}[\![\theta]\!]$. The proof is a structural induction on $\theta$. IH is short for induction hypothesis.

1. For any variable including $y$, $\mathsf{FV}(y) = \mathrm{FV}(y)$ since $y$ is the only variable that its value depends on.
2. $I\nu[\![f(\theta_1,\dots,\theta_k)]\!] \neq I\tilde{\nu}[\![f(\theta_1,\dots,\theta_k)]\!]$ implies for some $i$ that $I\nu[\![\theta_i]\!] \neq I\tilde{\nu}[\![\theta_i]\!]$. Hence, $y \in \mathsf{FV}(\theta_i)$ since $y$ is the only variable that $\nu$ and $\tilde{\nu}$ differ at. By IH, this implies $y \in \mathrm{FV}(\theta_i) \subseteq \mathrm{FV}(f(\theta_1,\dots,\theta_k))$. This includes the case where $f$ is $+$ or $\cdot$ as well.
3. $I\nu[\![(\theta)']\!] = \sum_x \nu(x') \frac{\partial I\nu[\![\theta]\!]}{\partial x} \neq \sum_x \tilde{\nu}(x') \frac{\partial I\tilde{\nu}[\![\theta]\!]}{\partial x} = I\tilde{\nu}[\![(\theta)']\!]$. Since $\nu$ and $\tilde{\nu}$ only differ in $y$, it is the case that *i)* for some $x$, $\frac{\partial I\nu[\![\theta]\!]}{\partial x} \neq \frac{\partial I\tilde{\nu}[\![\theta]\!]}{\partial x}$, or *ii)* $y$ is some $x'$ and $\nu(x') \neq \tilde{\nu}(x')$ and $\frac{\partial I\nu[\![\theta]\!]}{\partial x} \neq 0$ or $\frac{\partial I\tilde{\nu}[\![\theta]\!]}{\partial x} \neq 0$. In Case 3i, there are states $\omega = \tilde{\omega}$ that agree on $\{y\}^{\complement}$ such that $I\omega[\![\theta]\!] \neq I\tilde{\omega}[\![\theta]\!]$ as otherwise their partial derivatives by $x$ would agree. Thus, $y \in \mathsf{FV}(\theta) \overset{\text{IH}}{\subseteq} \mathrm{FV}(\theta) \subseteq \mathrm{FV}((\theta)')$ by IH. In Case 3ii, $x \in \mathsf{FV}(\theta)$ as, otherwise, $\frac{\partial I\nu[\![\theta]\!]}{\partial x} = 0$ for all states $\nu$ since there would not be any state $\omega$ agreeing $\omega = \nu$ on $\{x\}^{\complement}$ with a different value $I\omega[\![\theta]\!] \neq I\nu[\![\theta]\!]$ then, so that their partial derivatives by $x$ would both be 0. By IH, $x \in \mathsf{FV}(\theta)$ implies $x \in \mathrm{FV}(\theta)$, which implies $x' \in \mathrm{FV}((\theta)')$.

The proof of soundness of $\mathrm{FV}(\phi)$ and $\mathrm{FV}(\alpha)$ is indirect by a simultaneous inductive prove that both satisfy their respective coincidence property and are, thus, sound $\mathrm{FV}(\phi) \supseteq \mathsf{FV}(\phi)$ and $\mathrm{FV}(\alpha) \supseteq \mathsf{FV}(\alpha)$ by Lemmas 11 and 12, since $\mathsf{FV}(\phi)$ and $\mathsf{FV}(\alpha)$ are the smallest sets satisfying coincidence. In fact, the inductive proof for programs shows a stronger coincidence property augmented with must-bound variables.

The proof that $\mathrm{FV}(\phi)$ satisfies the coincidence property, and thus $\mathrm{FV}(\alpha) \supseteq \mathsf{FV}(\alpha)$, is by structural induction on $\phi$, simultaneously with the coincidence property for programs. To simplify the proof, doubly negated existential quantifiers are considered structurally smaller than universal quantifiers and doubly negated diamond modalities smaller than box modalities.

1. $\nu \in I[\![p(\theta_1,\dots,\theta_k)]\!]$ iff $(I\nu[\![\theta_1]\!],\dots,I\nu[\![\theta_k]\!]) \in I(p)$ iff $(J\tilde{\nu}[\![\theta_1]\!],\dots,J\tilde{\nu}[\![\theta_k]\!]) \in J(p)$ iff $\tilde{\nu} \in J[\![p(\theta_1,\dots,\theta_k)]\!]$ by Lemma 10 and $\mathrm{FV}(\theta) \supseteq \mathsf{FV}(\theta)$ since $\mathrm{FV}(\theta_i) \subseteq \mathrm{FV}(p(\theta_1,\dots,\theta_k))$ and $I$ and $J$ were assumed to agree on the function symbol $p$ that occurs in the formula. This includes the case where $p$ is $\geq$ so that $I$ and $J$ agree by definition.
2. $\nu \in I[\![C(\phi)]\!] = I(C)\big(I[\![\phi]\!]\big)$ iff, by IH, $\tilde{\nu} \in J[\![C(\phi)]\!] = J(C)\big(J[\![\phi]\!]\big)$ since $\nu = \tilde{\nu}$ on $\mathrm{FV}(C(\phi)) = \mathscr{V}$, so $\nu = \tilde{\nu}$, and $I = J$ on $\Sigma(C(\phi)) = \{C\} \cup \Sigma(\phi)$, so $I(C) = J(C)$ and, by induction hypothesis, implies $I[\![\phi]\!] = J[\![\phi]\!]$ using $I = J$ on $\Sigma(\phi) \subseteq \Sigma(C(\phi))$.
3. $\nu \in I[\![\neg\phi]\!]$ iff $\nu \notin I[\![\phi]\!]$ iff, by IH, $\tilde{\nu} \notin J[\![\phi]\!]$ iff $\tilde{\nu} \in J[\![\neg\phi]\!]$ using $\mathrm{FV}(\neg\phi) = \mathrm{FV}(\phi)$.
4. $\nu \in I[\![\phi \wedge \psi]\!]$ iff $\nu \in I[\![\phi]\!] \cap I[\![\psi]\!]$ iff, by IH, $\tilde{\nu} \in J[\![\phi]\!] \cap J[\![\psi]\!]$ iff $\tilde{\nu} \in J[\![\phi \wedge \psi]\!]$ using $\mathrm{FV}(\phi \wedge \psi) = \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi)$.
5. $\nu \in I[\![\exists x\, \phi]\!]$ iff $\nu_x^r \in I[\![\phi]\!]$ for some $r \in \mathbb{R}$ iff $\tilde{\nu}_x^r \in I[\![\phi]\!]$ for some $r \in \mathbb{R}$ iff $\tilde{\nu} \in J[\![\exists x\, \phi]\!]$ for the same $r$ by induction hypothesis using that $\nu_x^r = \tilde{\nu}_x^r$ on $\mathrm{FV}(\phi) \subseteq \{x\} \cup \mathrm{FV}(\exists x\, \phi)$.
6. The case $\forall x\, \phi$ follows from the equivalence $\forall x\, \phi \equiv \neg\exists x\, \neg\phi$ using $\mathrm{FV}(\neg\exists x\, \neg\phi) = \mathrm{FV}(\forall x\, \phi)$.

7. $\nu \in I[\![\langle\alpha\rangle\phi]\!]$ iff there is a $\omega$ such that $(\nu,\omega) \in I[\![\alpha]\!]$ and $\omega \in I[\![\phi]\!]$. Since $\nu = \tilde{\nu}$ on $\mathrm{FV}(\langle\alpha\rangle\phi) \supseteq \mathrm{FV}(\alpha)$ and $(\nu,\omega) \in I[\![\alpha]\!]$, the simultaneous induction hypothesis implies with $I = J$ on $\Sigma(\alpha) \subseteq \Sigma(\langle\alpha\rangle\phi)$ that there is an $\tilde{\omega}$ such that $(\tilde{\nu},\tilde{\omega}) \in J[\![\alpha]\!]$ and $\omega = \tilde{\omega}$ on $\mathrm{FV}(\langle\alpha\rangle\phi) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\phi) \cup \mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\phi)$.

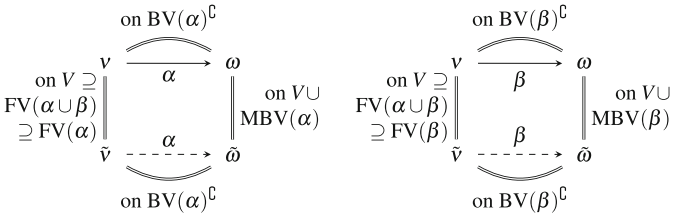
$$\begin{array}{ccc} \nu & \xrightarrow{\ \alpha\ } & \omega \\ \| & & \| \\ \tilde{\nu} & \xrightarrow{\ \alpha\ } & \tilde{\omega} \end{array} \quad \begin{array}{l} \text{on } \mathrm{FV}(\langle\alpha\rangle\phi) \\ \supseteq \mathrm{FV}(\alpha) \end{array} \qquad \text{on } \mathrm{FV}(\langle\alpha\rangle\phi) \cup \mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\phi)$$

   Since, $\omega = \tilde{\omega}$ on $\mathrm{FV}(\phi)$ and $I = J$ on $\Sigma(\phi) \subseteq \Sigma(\langle\alpha\rangle\phi)$, the induction hypothesis implies that $\tilde{\omega} \in J[\![\phi]\!]$ since $\omega \in I[\![\phi]\!]$. Since $(\tilde{\nu},\tilde{\omega}) \in J[\![\alpha]\!]$, this implies $\tilde{\nu} \in J[\![\langle\alpha\rangle\phi]\!]$.
8. $\nu \in I[\![[\alpha]\phi]\!] = I[\![\neg\langle\alpha\rangle\neg\phi]\!]$ iff $\nu \notin I[\![\langle\alpha\rangle\neg\phi]\!]$, so by IH, iff $\tilde{\nu} \notin J[\![\langle\alpha\rangle\neg\phi]\!]$ iff $\tilde{\nu} \in J[\![[\alpha]\phi]\!]$ using that $\mathrm{FV}(\langle\alpha\rangle\neg\phi) = \mathrm{FV}([\alpha]\phi)$.

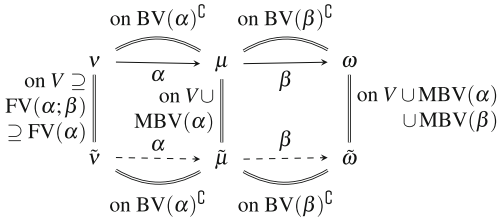
The proof that $\mathrm{FV}(\alpha)$ satisfies the coincidence property, and thus $\mathrm{FV}(\phi) \supseteq \mathsf{FV}(\phi)$, shows a stronger property. If $\nu = \tilde{\nu}$ on $V \supseteq \mathrm{FV}(\alpha)$, $I = J$ on $\Sigma(\alpha)$ and $(\nu,\omega) \in I[\![\alpha]\!]$, then there is a $\tilde{\omega}$ such that $(\tilde{\nu},\tilde{\omega}) \in J[\![\alpha]\!]$ and $\omega = \tilde{\omega}$ on $V \cup \mathrm{MBV}(\alpha)$. The proof is by (simultaneous) induction on the structural complexity of $\alpha$, where $\alpha^*$ is considered to be structurally more complex than HPs of any length but with less nested repetitions, which induces a well-founded order on HPs. For atomic programs $\alpha$ for which $\mathrm{BV}(\alpha) = \mathrm{MBV}(\alpha)$, it is enough to show agreement on $\mathrm{V}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{BV}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{MBV}(\alpha)$, because any variable in $V \setminus \mathrm{V}(\alpha)$ is in $\mathrm{BV}(\alpha)^{\complement}$, which remain unchanged by $\alpha$ according to Lemma 9 and $\mathrm{BV}(\alpha) \supseteq \mathsf{BV}(\alpha)$.

1. Since $\mathrm{FV}(a) = \mathscr{V}$ so $\nu = \tilde{\nu}$, the statement is vacuously true for program constant $a$.
2. $(\nu,\omega) \in I[\![x := \theta]\!] = \{(\nu,\omega) : \omega = \nu \text{ except that } I\omega[\![x]\!] = I\nu[\![\theta]\!]\}$ then there is $(\tilde{\nu},\tilde{\omega}) \in J[\![x := \theta]\!]$ and $\tilde{\omega}(x) = J\tilde{\omega}[\![x]\!] = J\tilde{\nu}[\![\theta]\!] = I\nu[\![\theta]\!] = I\omega[\![x]\!] = \nu(x)$ by Lemma 10, since $\nu = \tilde{\nu}$ on $\mathrm{FV}(x := \theta) = \mathrm{FV}(\theta)$ and $I = J$ on $\Sigma(\theta)$. So, $\omega = \tilde{\omega}$ on $\mathrm{BV}(x := \theta) = \{x\}$. Also, $\nu = \omega$ on $\mathrm{BV}(x := \theta)^{\complement}$ and $\tilde{\nu} = \tilde{\omega}$ on $\mathrm{BV}(x := \theta)^{\complement}$ by Lemma 9. Since $\nu = \tilde{\nu}$ on $\mathrm{FV}(x := \theta)$, these imply $\omega = \tilde{\omega}$ on $\mathrm{FV}(x := \theta) \setminus \mathrm{BV}(x := \theta)$. Since $\omega = \tilde{\omega}$ on $\mathrm{BV}(x := \theta)$ had been shown already, this implies $\omega = \tilde{\omega}$ on $\mathrm{V}(x := \theta)$.
3. $(\nu,\omega) \in I[\![?\psi]\!] = \{(\nu,\nu) : \nu \in I[\![\psi]\!]\}$ then $\omega = \nu$ by Definition 7. Since, $\nu \in I[\![\psi]\!]$ and $\nu = \tilde{\nu}$ on $\mathrm{FV}(?\psi)$ and $I = J$ on $\Sigma(?\psi) = \Sigma(?\psi)$, Lemma 11 and the simultaneous induction for $\mathrm{FV}(\psi) \supseteq \mathsf{FV}(\psi)$ implies that $\tilde{\nu} \in J[\![\psi]\!]$, so $(\tilde{\nu},\tilde{\nu}) \in J[\![?\psi]\!]$. So $\nu = \tilde{\nu}$ on $\mathrm{V}(?\psi) = \mathrm{FV}(?\psi)$ since $\mathrm{BV}(?\psi) = \emptyset$.
4. $(\nu,\omega) \in I[\![x' = \theta \,\&\, \psi]\!]$ implies that there is an $\tilde{\omega}$ reached from $\tilde{\nu}$ by following the differential equation for the same amount it took to reach $\omega$ from $\nu$.
   That is, $\nu = \varphi(0)$ on $\{x'\}^{\complement}$ and $\omega = \varphi(r)$ for some function $\varphi : [0,r] \to \mathscr{S}$ satisfying $I, \varphi \models x' = \theta \wedge \psi$, especially $\varphi(\zeta) \in I[\![x' = \theta \wedge \psi]\!]$ for all $0 \leq \zeta \leq r$. Define $\tilde{\varphi} : [0,r] \to \mathscr{S}$ at $\zeta$ as $\tilde{\varphi}(\zeta) = \varphi(\zeta)$ on $\{x,x'\}$ and as $\tilde{\varphi}(\zeta) = \tilde{\nu}$ on $\{x,x'\}^{\complement}$. Fix any $0 \leq \zeta \leq r$. Then it only remains to show that $\tilde{\varphi}(\zeta) \in J[\![x' = \theta \wedge \psi]\!]$, i.e. $\tilde{\varphi}(\zeta) \in J[\![x' = \theta]\!] \cap J[\![\psi]\!]$, which follows from $\varphi(\zeta) \in I[\![x' = \theta]\!] \cap I[\![\psi]\!]$ by Lemma 11 and the simultaneous induction hypothesis, since $I = J$ on $\Sigma(x' = \theta) \cup \Sigma(\psi) = \Sigma(x' = \theta \,\&\, \psi)$ and $\varphi(\zeta) = \tilde{\varphi}(\zeta)$ on $\mathrm{FV}(x' = \theta) \cup \mathrm{FV}(\psi) = \mathrm{FV}(x' = \theta \,\&\, \psi) \cup \{x'\}$. Here, $\varphi(\zeta) = \tilde{\varphi}(\zeta)$ agree on $\{x,x'\}$ by construction of $\tilde{\varphi}$. Agreement of $\varphi(\zeta)$ and $\tilde{\varphi}(\zeta)$ for the other free variables follows from the assumption that $\nu = \tilde{\nu}$ on $\mathrm{FV}(x' = \theta \,\&\, \psi)$ since $\nu = \varphi(\zeta)$ on $\{x,x'\}^{\complement}$ by Definition 7 and since $\tilde{\nu} = \tilde{\varphi}(\zeta)$ on $\{x,x'\}^{\complement}$ by construction.
5. $(\nu,\omega) \in I[\![\alpha \cup \beta]\!] = I[\![\alpha]\!] \cup I[\![\beta]\!]$ implies $(\nu,\omega) \in I[\![\alpha]\!]$ or $(\nu,\omega) \in I[\![\beta]\!]$, which since $V \supseteq \mathrm{FV}(\alpha \cup \beta) \supseteq \mathrm{FV}(\alpha)$ and $V \supseteq \mathrm{FV}(\alpha \cup \beta) \supseteq \mathrm{FV}(\beta)$ implies, by induction hypothesis, that there is an $\tilde{\omega}$ such that $(\tilde{\nu},\tilde{\omega}) \in J[\![\alpha]\!]$ and $\omega = \tilde{\omega}$ on $V \cup \mathrm{MBV}(\alpha)$

or that there is an $\tilde{\omega}$ such that $(\tilde{\nu},\tilde{\omega}) \in J[\![\beta]\!]$ and $\omega = \tilde{\omega}$ on $V \cup \mathrm{MBV}(\beta)$, respectively. In either case, there is a $\tilde{\omega}$ such that $(\tilde{\nu},\tilde{\omega}) \in J[\![\alpha \cup \beta]\!]$ and $\omega = \tilde{\omega}$ on $V \cup \mathrm{MBV}(\alpha \cup \beta)$, because $J[\![\alpha]\!] \subseteq J[\![\alpha \cup \beta]\!]$ and $J[\![\beta]\!] \subseteq J[\![\alpha \cup \beta]\!]$ and $\mathrm{MBV}(\alpha \cup \beta) = \mathrm{MBV}(\alpha) \cap \mathrm{MBV}(\beta)$.




6. $(\nu,\omega) \in I[\![\alpha;\beta]\!] = I[\![\alpha]\!] \circ I[\![\beta]\!]$, i.e. there is a state $\mu$ such that $(\nu,\mu) \in I[\![\alpha]\!]$ and $(\mu,\omega) \in I[\![\beta]\!]$. Since $V \supseteq \mathrm{FV}(\alpha;\beta) \supseteq \mathrm{FV}(\alpha)$, by induction hypothesis, there is a $\tilde{\mu}$ such that $(\tilde{\nu},\tilde{\mu}) \in J[\![\alpha]\!]$ and $\mu = \tilde{\mu}$ on $V \cup \mathrm{MBV}(\alpha)$. Since $V \supseteq \mathrm{FV}(\alpha;\beta)$, so $V \cup \mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\alpha;\beta) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\alpha) = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta) \cup \mathrm{MBV}(\alpha) \supseteq \mathrm{FV}(\beta)$ by Definition 15, and since $(\mu,\omega) \in I[\![\beta]\!]$, the induction hypothesis implies that there is an $\tilde{\omega}$ such that $(\tilde{\mu},\tilde{\omega}) \in J[\![\beta]\!]$ and $\omega = \tilde{\omega}$ on $(V \cup \mathrm{MBV}(\alpha)) \cup \mathrm{MBV}(\beta) = V \cup \mathrm{MBV}(\alpha;\beta)$.




7. $(\nu,\omega) \in I[\![\alpha^*]\!] = \bigcup_{n\in\mathbb{N}} I[\![\alpha^n]\!]$ iff there is an $n \in \mathbb{N}$ such that $(\nu,\omega) \in I[\![\alpha^n]\!]$. The case $n = 0$ follows from the assumption $\nu = \tilde{\nu}$ on $V \supseteq \mathrm{FV}(\alpha)$, since $\omega = \nu$ holds in that case and $\mathrm{MBV}(\alpha^*) = \emptyset$. The case $n > 0$ proceeds as follows. Since $\mathrm{FV}(\alpha^n) = \mathrm{FV}(\alpha^*) = \mathrm{FV}(\alpha)$, the induction hypothesis applied to the structurally simpler HP $\alpha^n \equiv \alpha^{n-1};\alpha$ with less loops (so using Case 6) implies that there is an $\tilde{\omega}$ such that $(\tilde{\nu},\tilde{\omega}) \in J[\![\alpha^n]\!]$ and $\omega = \tilde{\omega}$ on $V \cup \mathrm{MBV}(\alpha^n) \supseteq V = V \cup \mathrm{MBV}(\alpha^*)$, since $\mathrm{MBV}(\alpha^*) = \emptyset$. Since $J[\![\alpha^n]\!] \subseteq J[\![\alpha^*]\!]$ by Definition 7, this concludes the proof. □

*Proof of Corollary 22.* $\sigma_\nu^* I$ is well-defined, as $\sigma_\nu^* I(f)$ is a smooth function since its substitute term $\sigma f(\cdot)$ has smooth values. First, $\sigma_\nu^* I(a) = I[\![\sigma a]\!] = \sigma_\omega^* I(a)$ holds because the adjoint to $\sigma$ for $I$, $\nu$ in the case of programs is independent of $\nu$ (programs have access to their initial state at runtime). Likewise $\sigma_\nu^* I(C) = \sigma_\omega^* I(C)$ for quantifier symbols, because the adjoint is independent of $\nu$ for quantifier symbols. By Lemma 10, $I_{\cdot}^d \nu[\![\sigma f(\cdot)]\!] = I_{\cdot}^d \omega[\![\sigma f(\cdot)]\!]$ when $\nu = \omega$ on $\mathsf{FV}(\sigma f(\cdot)) \subseteq \mathsf{FV}(\sigma)$. Also $\nu \in I_{\cdot}^d[\![\sigma p(\cdot)]\!]$ iff $\omega \in I_{\cdot}^d[\![\sigma p(\cdot)]\!]$ by Lemma 11 when $\nu = \omega$ on $\mathsf{FV}(\sigma p(\cdot)) \subseteq \mathsf{FV}(\sigma)$. Thus, $\sigma_\nu^* I = \sigma_\omega^* I$ when $\nu = \omega$ on $\mathsf{FV}(\sigma)$.

If $\sigma$ is $U$-admissible for $\phi$ (or $\theta$ or $\alpha$), then $\mathsf{FV}(\sigma f(\cdot)) \cap U = \emptyset$, i.e. $\mathsf{FV}(\sigma f(\cdot)) \subseteq U^{\complement}$ for every function symbol $f \in \Sigma(\phi)$ (or $\theta$ or $\alpha$) and likewise for predicate symbols $p \in \Sigma(\phi)$. Since $\nu = \omega$ on $U^{\complement}$ was assumed, $\sigma_\omega^* I = \sigma_\nu^* I$ on the function and predicate symbols in $\Sigma(\phi)$ (or $\theta$ or $\alpha$). Finally $\sigma_\omega^* I = \sigma_\nu^* I$ on $\Sigma(\phi)$ (or $\Sigma(\theta)$ or $\Sigma(\alpha)$, respectively) implies

that $\sigma_\omega^* I[\![\phi]\!] = \sigma_\nu^* I[\![\phi]\!]$ by Lemma 11 (since $\mu \in \sigma_\omega^* I[\![\phi]\!]$ iff $\mu \in \sigma_\nu^* I[\![\phi]\!]$ holds for all $\mu$) and that $\sigma_\nu^* I[\![\theta]\!] = \sigma_\omega^* I[\![\theta]\!]$ by Lemma 10 and that $\sigma_\omega^* I[\![\alpha]\!] = \sigma_\nu^* I[\![\alpha]\!]$ by Lemma 12, respectively. □

*Proof of Lemma 23.* The proof is by structural induction on $\theta$ and the structure of $\sigma$.

1. $I\nu[\![\sigma(x)]\!] = I\nu[\![x]\!] = \nu(x) = \sigma_\nu^* I\nu[\![x]\!]$ since $x \notin \sigma$ for variable $x \in \mathscr{V}$
2. Let $f \in \sigma$. Then $I\nu[\![\sigma(f(\theta))]\!] = I\nu[\![(\sigma(f))\big(\sigma(\theta)\big)]\!] = I\nu[\![\{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))]\!] \overset{\text{IH}}{=} I^d_{\cdot}\nu[\![\sigma f(\cdot)]\!] = (\sigma_\nu^* I(f))(d) = (\sigma_\nu^* I(f))(\sigma_\nu^* I\nu[\![\theta]\!]) = \sigma_\nu^* I\nu[\![f(\theta)]\!]$ with $d \overset{\text{def}}{=} I\nu[\![\sigma(\theta)]\!] \overset{\text{IH}}{=} \sigma_\nu^* I\nu[\![\theta]\!]$ by using the induction hypothesis twice, once for $\sigma(\theta)$ on the smaller $\theta$ and once for $\{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot))$ on the possibly bigger term $\sigma f(\cdot)$ but the structurally simpler uniform substitution $\{\cdot \mapsto \sigma(\theta)\}(\dots)$ that is a substitution on the symbol $\cdot$ of arity zero, not a substitution of functions with arguments. For well-foundedness of the induction note that the $\cdot$ substitution only happens for function symbols $f$ with at least one argument $\theta$ so not for $\cdot$ itself.
3. $I\nu[\![\sigma(g(\theta))]\!] = I\nu[\![g(\sigma(\theta))]\!] = I(g)\big(I\nu[\![\sigma(\theta)]\!]\big) \overset{\text{IH}}{=} I(g)\big(\sigma_\nu^* I\nu[\![\theta]\!]\big) = \sigma_\nu^* I(g)\big(\sigma_\nu^* I\nu[\![\theta]\!]\big) = \sigma_\nu^* I\nu[\![g(\theta)]\!]$ by induction hypothesis and since $I(g) = \sigma_\nu^* I(g)$ as the interpretation of $g$ does not change in $\sigma_\nu^* I$ when $g \notin \sigma$.
4. $I\nu[\![\sigma(\theta+\eta)]\!] = I\nu[\![\sigma(\theta)+\sigma(\eta)]\!] = I\nu[\![\sigma(\theta)]\!] + I\nu[\![\sigma(\eta)]\!] \overset{\text{IH}}{=} \sigma_\nu^* I\nu[\![\theta]\!] + \sigma_\nu^* I\nu[\![\eta]\!] = \sigma_\nu^* I\nu[\![\theta+\eta]\!]$ by induction hypothesis.
5. $I\nu[\![\sigma(\theta\cdot\eta)]\!] = I\nu[\![\sigma(\theta)\cdot\sigma(\eta)]\!] = I\nu[\![\sigma(\theta)]\!] \cdot I\nu[\![\sigma(\theta)]\!] \overset{\text{IH}}{=} \sigma_\nu^* I\nu[\![\theta]\!] \cdot \sigma_\nu^* I\nu[\![\eta]\!] = \sigma_\nu^* I\nu[\![\theta\cdot\eta]\!]$ by induction hypothesis.
6. $I\nu[\![\sigma((\theta)')]\!] = I\nu[\![(\sigma(\theta))']\!] = \sum_x \nu(x') \frac{\partial I\nu[\![\sigma(\theta)]\!]}{\partial x} \overset{\text{IH}}{=} \sum_x \nu(x') \frac{\partial \sigma_\nu^* I\nu[\![\theta]\!]}{\partial x} = \sigma_\nu^* I\nu[\![(\theta)']\!]$ by induction hypothesis, provided $\sigma$ is $\mathscr{V}$-admissible for $\theta$, i.e. does not introduce any variables or differential symbols, so that Corollary 22 implies $\sigma_\nu^* I = \sigma_\omega^* I$ for all $\nu, \omega$ (that agree on $\mathscr{V}^{\complement} = \emptyset$, which imposes no condition on $\nu, \omega$). In particular, the adjoint interpretation $\sigma_\nu^* I$ is the same for all ways of changing the value of variable $x$ in state $\nu$ when forming the partial derivative. □

*Proof of Lemma 24.* The proof is by structural induction on $\phi$ and the structure on $\sigma$, simultaneously with Lemma 25.

1. $\nu \in I[\![\sigma(\theta \geq \eta)]\!]$ iff $\nu \in I[\![\sigma(\theta) \geq \sigma(\eta)]\!]$ iff $I\nu[\![\sigma(\theta)]\!] \geq I\nu[\![\sigma(\eta)]\!]$, by Lemma 23, iff $\sigma_\nu^* I\nu[\![\theta]\!] \geq \sigma_\nu^* I\nu[\![\eta]\!]$ iff $\sigma_\nu^* I\nu[\![\theta \geq \eta]\!]$.
2. Let $p \in \sigma$. Then $\nu \in I[\![\sigma(p(\theta))]\!]$ iff $\nu \in I[\![(\sigma(p))\big(\sigma(\theta)\big)]\!]$ iff $\nu \in I[\![\{\cdot \mapsto \sigma(\theta)\}(\sigma p(\cdot))]\!]$ iff, by IH, $\nu \in I^d_{\cdot}[\![\sigma p(\cdot)]\!]$ iff $d \in \sigma_\nu^* I(p)$ iff $(\sigma_\nu^* I\nu[\![\theta]\!]) \in \sigma_\nu^* I(p)$ iff $\nu \in \sigma_\nu^* I[\![p(\theta)]\!]$ with $d \overset{\text{def}}{=} I\nu[\![\sigma(\theta)]\!] = \sigma_\nu^* I\nu[\![\theta]\!]$ by using Lemma 23 for $\sigma(\theta)$ and by using the induction hypothesis for $\{\cdot \mapsto \sigma(\theta)\}(\sigma p(\cdot))$ on the possibly bigger formula $\sigma p(\cdot)$ but the structurally simpler uniform substitution $\{\cdot \mapsto \sigma(\theta)\}(\dots)$ that is a mere substitution on function symbol $\cdot$ of arity zero, not a substitution of predicates.
3. Let $q \notin \sigma$. Then $\nu \in I[\![\sigma(q(\theta))]\!]$ iff $\nu \in I[\![q(\sigma(\theta))]\!]$ iff $\big(I\nu[\![\sigma(\theta)]\!]\big) \in I(q)$ so, by Lemma 23, that holds iff $\big(\sigma_\nu^* I\nu[\![\theta]\!]\big) \in I(q)$ iff $\big(\sigma_\nu^* I\nu[\![\theta]\!]\big) \in \sigma_\nu^* I(q)$ iff $\nu \in \sigma_\nu^* I[\![q(\theta)]\!]$ since $I(q) = \sigma_\nu^* I(q)$ as the interpretation of $q$ does not change in $\sigma_\nu^* I$ when $q \notin \sigma$.
4. For the case $\sigma(C(\phi))$, first show $I[\![\sigma(\phi)]\!] = \sigma_\nu^* I[\![\phi]\!]$. By induction hypothesis for the smaller $\phi$: $\omega \in I[\![\sigma(\phi)]\!]$ iff $\omega \in \sigma_\omega^* I[\![\phi]\!]$, where $\sigma_\omega^* I[\![\phi]\!] = \sigma_\nu^* I[\![\phi]\!]$ by Corollary 22 for all $\nu, \omega$ (that agree on $\mathscr{V}^{\complement} = \emptyset$, which imposes no condition on $\nu, \omega$) since $\sigma$ is $\mathscr{V}$-admissible for $\phi$. The proof proceeds: $\nu \in I[\![\sigma(C(\phi))]\!] = I[\![\sigma(C)(\sigma(\phi))]\!] = I[\![\{\_ \mapsto \sigma(\phi)\}(\sigma C(\_))]\!]$, so, by induction hypothesis for the structurally simpler uniform substitution $\{\_ \mapsto \sigma(\phi)\}$ that is a mere substitution on quantifier symbol $\_$ of arity

zero, iff $\nu \in I^R_{\_}[\![\sigma C(\_)]\!]$ since the adjoint to $\{\_ \mapsto \sigma(\phi)\}$ is $I^R_{\_}$ with $R \overset{\text{def}}{=} I[\![\sigma(\phi)]\!]$ by definition.
Also $\nu \in \sigma^*_\nu I[\![C(\phi)]\!] = \sigma^*_\nu I(C)\big(\sigma^*_\nu I[\![\phi]\!]\big) = I^R_{\_}[\![\sigma C(\_)]\!]$ for $R = \sigma^*_\nu I[\![\phi]\!] = I[\![\sigma(\phi)]\!]$ by induction hypothesis. Both sides are, thus, equivalent.

5. The case $\sigma(C(\phi))$ for $C \notin \sigma$ again first shows $I[\![\sigma(\phi)]\!] = \sigma^*_\nu I[\![\phi]\!]$ for all $\nu$ using that $\sigma$ is $\mathscr{V}$-admissible for $\phi$. Then $\nu \in I[\![\sigma(C(\phi))]\!] = I[\![C(\sigma(\phi))]\!] = I(C)\big(I[\![\sigma(\phi)]\!]\big) = I(C)\big(\sigma^*_\nu I[\![\phi]\!]\big) = \sigma^*_\nu I(C)\big(\sigma^*_\nu I[\![\phi]\!]\big) = \sigma^*_\nu I[\![C(\phi)]\!]$ iff $\nu \in \sigma^*_\nu I[\![C(\phi)]\!]$
6. $\nu \in I[\![\sigma(\neg\phi)]\!]$ iff $\nu \in I[\![\neg\sigma(\phi)]\!]$ iff $\nu \notin I[\![\sigma(\phi)]\!]$, so by IH, iff $\nu \notin \sigma^*_\nu I[\![\phi]\!]$ iff $\nu \in \sigma^*_\nu I[\![\neg\phi]\!]$
7. $\nu \in I[\![\sigma(\phi \wedge \psi)]\!]$ iff $\nu \in I[\![\sigma(\phi) \wedge \sigma(\psi)]\!]$ iff $\nu \in I[\![\sigma(\phi)]\!]$ and $\nu \in I[\![\sigma(\psi)]\!]$, by induction hypothesis, iff $\nu \in \sigma^*_\nu I[\![\phi]\!]$ and $\nu \in \sigma^*_\nu I[\![\psi]\!]$ iff $\nu \in \sigma^*_\nu I[\![\phi \wedge \psi]\!]$
8. $\nu \in I[\![\sigma(\exists x\, \phi)]\!]$ iff $\nu \in I[\![\exists x\, \sigma(\phi)]\!]$ (provided that $\sigma$ is $\{x\}$-admissible for $\phi$) iff $\nu^d_x \in I[\![\sigma(\phi)]\!]$ for some $d$, so, by induction hypothesis, iff $\nu^d_x \in \sigma^*_{\nu^d_x} I[\![\phi]\!]$ for some $d$, which is equivalent to $\nu^d_x \in \sigma^*_\nu I[\![\phi]\!]$ by Corollary 22 as $\sigma$ is $\{x\}$-admissible for $\phi$ and $\nu = \nu^d_x$ on $\{x\}^{\complement}$. Thus, this is equivalent to $\nu \in \sigma^*_\nu I[\![\exists x\, \phi]\!]$.
9. The case $\nu \in I[\![\sigma(\forall x\, \phi)]\!]$ follows by duality $\forall x\, \phi \equiv \neg\exists x\, \neg\phi$, which is respected in the definition of uniform substitutions.
10. $\nu \in I[\![\sigma(\langle\alpha\rangle\phi)]\!]$ iff $\nu \in I[\![\langle\sigma(\alpha)\rangle\sigma(\phi)]\!]$ (provided $\sigma$ is $\mathsf{BV}(\sigma(\alpha))$-admissible for $\phi$) iff there is a $\omega$ such that $(\nu, \omega) \in I[\![\sigma(\alpha)]\!]$ and $\omega \in I[\![\sigma(\phi)]\!]$, which, by Lemma 25 and induction hypothesis, respectively, is equivalent to: there is a $\omega$ such that $(\nu, \omega) \in \sigma^*_\nu I[\![\alpha]\!]$ and $\omega \in \sigma^*_\omega I[\![\phi]\!]$, which is equivalent to $\nu \in \sigma^*_\nu I[\![\langle\alpha\rangle\phi]\!]$, because $\omega \in \sigma^*_\omega I[\![\phi]\!]$ is equivalent to $\omega \in \sigma^*_\nu I[\![\phi]\!]$ by Corollary 22 as $\sigma$ is $\mathsf{BV}(\sigma(\alpha))$-admissible for $\phi$ and $\nu = \omega$ on $\mathsf{BV}(\sigma(\alpha))^{\complement}$ by Lemma 9 since $(\nu, \omega) \in I[\![\sigma(\alpha)]\!]$.
11. The case $\nu \in I[\![\sigma([\alpha]\phi)]\!]$ follows by duality $[\alpha]\phi \equiv \neg\langle\alpha\rangle\neg\phi$, which is respected in the definition of uniform substitutions. □

*Proof of Lemma 25.* The proof is by structural induction on $\alpha$, simultaneously with Lemma 24.

1. $(\nu, \omega) \in I[\![\sigma(a)]\!] = I[\![\sigma a]\!] = \sigma^*_\nu I(a) = \sigma^*_\nu I[\![a]\!]$ for program constant $a \in \sigma$ (the proof is accordingly for $a \notin \sigma$).
2. $(\nu, \omega) \in I[\![\sigma(x := \theta)]\!] = I[\![x := \sigma(\theta)]\!]$ iff $\omega = \nu^{I\nu[\![\sigma(\theta)]\!]}_x = \nu^{\sigma^*_\nu I\nu[\![\theta]\!]}_x$ by Lemma 24, which is, thus, equivalent to $(\nu, \omega) \in \sigma^*_\nu I[\![x := \theta]\!]$.
3. $(\nu, \omega) \in I[\![\sigma(?\psi)]\!] = I[\![?\sigma(\psi)]\!]$ iff $\omega = \nu$ and $\nu \in I[\![\sigma(\psi)]\!]$, iff, by Lemma 24, $\omega = \nu$ and $\nu \in \sigma^*_\nu I[\![\psi]\!]$, which is equivalent to $(\nu, \omega) \in \sigma^*_\nu I[\![?\psi]\!]$.
4. $(\nu, \omega) \in I[\![\sigma(x' = \theta \,\&\, \psi)]\!] = I[\![x' = \sigma(\theta) \,\&\, \sigma(\psi)]\!]$ (provided that $\sigma$ is $\{x, x'\}$-admissible for $\theta$, $\psi$) iff $\exists\varphi : [0, T] \to \mathscr{S}$ with $\varphi(0) = \nu$ on $\{x'\}^{\complement}$, $\varphi(T) = \omega$ and for all $t \geq 0$: $\varphi'(t) = I\varphi(t)[\![\sigma(\theta)]\!] = \sigma^*_{\varphi(t)} I\varphi(t)[\![\theta]\!]$ by Lemma 23 and $\varphi(t) \in I[\![\sigma(\psi)]\!]$, which, by Lemma 24, holds iff $\varphi(t) \in \sigma^*_{\varphi(t)} I[\![\psi]\!]$.

   Also $(\nu, \omega) \in \sigma^*_\nu I[\![x' = \theta \,\&\, \psi]\!]$ iff $\exists\varphi : [0, T] \to \mathscr{S}$ with $\varphi(0) = \nu$ on $\{x'\}^{\complement}$ and $\varphi(T) = \omega$ and for all $t \geq 0$: $\varphi'(t) = \sigma^*_\nu I\varphi(t)[\![\theta]\!]$ and $\varphi(t) \in \sigma^*_\nu I[\![\psi]\!]$. Finally, $\sigma^*_\nu I[\![\theta]\!] = \sigma^*_{\varphi(t)} I[\![\theta]\!]$ and $\sigma^*_{\varphi(t)} I[\![\psi]\!] = \sigma^*_\nu I[\![\psi]\!]$ by Corollary 22 since $\sigma$ is $\{x, x'\}$-admissible for $\theta$ and $\psi$ and $\nu = \varphi(t)$ on $\mathsf{BV}(x' = \theta \,\&\, \psi)^{\complement} \supseteq \{x, x'\}^{\complement}$ by Lemma 9.
5. $(\nu, \omega) \in I[\![\sigma(\alpha \cup \beta)]\!] = I[\![\sigma(\alpha) \cup \sigma(\beta)]\!] = I[\![\sigma(\alpha)]\!] \cup I[\![\sigma(\beta)]\!]$, which, by induction hypothesis, is equivalent to $(\nu, \omega) \in \sigma^*_\nu I[\![\alpha]\!]$ or $(\nu, \omega) \in \sigma^*_\nu I[\![\beta]\!]$, which is $(\nu, \omega) \in \sigma^*_\nu I[\![\alpha]\!] \cup \sigma^*_\nu I[\![\beta]\!] = \sigma^*_\nu I[\![\alpha \cup \beta]\!]$.
6. $(\nu, \omega) \in I[\![\sigma(\alpha; \beta)]\!] = I[\![\sigma(\alpha); \sigma(\beta)]\!] = I[\![\sigma(\alpha)]\!] \circ I[\![\sigma(\beta)]\!]$ (provided $\sigma$ is $\mathsf{BV}(\sigma(\alpha))$-admissible for $\beta$) iff there is a $\mu$ such that $(\nu, \mu) \in I[\![\sigma(\alpha)]\!]$ and $(\mu, \omega) \in I[\![\sigma(\beta)]\!]$,

which, by induction hypothesis, is equivalent to $(\nu,\mu)\in\sigma^*_\nu I[\![\alpha]\!]$ and $(\mu,\omega)\in\sigma^*_\mu I[\![\beta]\!]$. Yet, $\sigma^*_\mu I[\![\beta]\!]=\sigma^*_\nu I[\![\beta]\!]$ by Corollary 22, because $\sigma$ is $\mathsf{BV}(\sigma(\alpha))$-admissible for $\beta$ and $\nu=\omega$ on $\mathsf{BV}(\sigma(\alpha))^{\complement}$ by Lemma 9 since $(\nu,\mu)\in I[\![\sigma(\alpha)]\!]$. Finally, $(\nu,\mu)\in\sigma^*_\nu I[\![\alpha]\!]$ and $(\mu,\omega)\in\sigma^*_\nu I[\![\beta]\!]$ for some $\mu$ is equivalent to $(\nu,\omega)\in\sigma^*_\nu I[\![\alpha;\beta]\!]$.

7. $(\nu,\omega)\in I[\![\sigma(\alpha^*)]\!]=I[\![(\sigma(\alpha))^*]\!]=\big(I[\![\sigma(\alpha)]\!]\big)^*=\bigcup_{n\in\mathbb{N}}(I[\![\sigma(\alpha)]\!])^n$ (provided that $\sigma$ is $\mathsf{BV}(\sigma(\alpha))$-admissible for $\alpha$) iff there are $n\in\mathbb{N}$ and $\nu_0=\nu,\nu_1,\dots,\nu_n=\omega$ such that $(\nu_i,\nu_{i+1})\in I[\![\sigma(\alpha)]\!]$ for all $i<n$. By $n$ uses of the induction hypothesis, this is equivalent to $(\nu_i,\nu_{i+1})\in\sigma^*_{\nu_i}I[\![\alpha]\!]$ for all $i<n$, which is equivalent to $(\nu_i,\nu_{i+1})\in\sigma^*_\nu I[\![\alpha]\!]$ by Corollary 22 since $\sigma$ is $\mathsf{BV}(\sigma(\alpha))$-admissible for $\alpha$ and $\nu_{i+1}=\nu_i$ on $\mathsf{BV}(\sigma(\alpha))^{\complement}$ by Lemma 9 as $(\nu_i,\nu_{i+1})\in I[\![\sigma(\alpha)]\!]$ for all $i<n$. Thus, this is equivalent to $(\nu,\omega)\in\sigma^*_\nu I[\![\alpha^*]\!]=\big(\sigma^*_\nu I[\![\alpha]\!]\big)^*$. □

*Proof of Lemma 35.* By Definition 5 the left side is:

$$I\varphi(\zeta)[\![(\eta)']\!]=\sum_{x\in\mathscr{V}}\varphi(\zeta)(x')\frac{\partial I[\![\eta]\!]}{\partial x}(\varphi(\zeta))$$

By chain rule (Lemma 42 in the beginning of the "Appendix") the right side is:

$$\frac{\mathsf{d}I\varphi(t)[\![\eta]\!]}{\mathsf{d}t}(\zeta)=(I[\![\eta]\!]\circ\varphi)'(\zeta)=(\nabla I[\![\eta]\!])\big(\varphi(\zeta)\big)\cdot\varphi'(\zeta)=\sum_{x\in\mathscr{V}}\frac{\partial I[\![\eta]\!]}{\partial x}\big(\varphi(\zeta)\big)\varphi'(\zeta)(x)$$

where $(\nabla I[\![\eta]\!])\big(\varphi(\zeta)\big)$, the gradient $\nabla I[\![\eta]\!]$ of $I[\![\eta]\!]$ at $\varphi(\zeta)$, is the vector of $\frac{\partial I[\![\eta]\!]}{\partial x}\big(\varphi(\zeta)\big)$, which has finite support by Lemma 10 so is 0 for all but finitely many variables. Both sides, thus, agree since $\varphi(\zeta)(x')=\frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(\zeta)=\varphi'(\zeta)(x)$ by Definition 7 for all $x\in\mathsf{FV}(\eta)$. The same proof works for vectorial differential equations as long as all free variables of $\eta$ have some differential equation so that their differential symbols agree with their time-derivatives. □

*Proof of Lemma 36.* $I,\varphi\models x'=\theta\wedge\psi$ implies $\varphi(\zeta)\in I[\![x'=\theta\wedge\psi]\!]$, i.e. $\varphi(\zeta)(x')=I\varphi(\zeta)[\![\theta]\!]$ and also $\varphi(\zeta)\in I[\![\psi]\!]$ for all $0\leq\zeta\leq r$. Thus, since $x'$ already has the value $I\varphi(\zeta)[\![\theta]\!]$ in state $\varphi(\zeta)$, the differential assignment $x':=\theta$ has no effect, thus, $(\varphi(\zeta),\varphi(\zeta))\in I[\![x':=\theta]\!]$ so that $\phi$ and $[x':=\theta]\phi$ are equivalent along $\varphi$. Hence, $I,\varphi\models(\phi\leftrightarrow[x':=\theta]\phi)$. □

*Proof of Lemma 37.* The proof shows each equation separately. The first part considers any constant function (i.e. arity 0) or number literal $f$ for (3) and then aligns the differential $(x)'$ of a term that happens to be a variable $x\in\mathscr{V}$ with its corresponding differential symbol $x'\in\mathscr{V}'$ for (4). The other cases exploit linearity for (5) and Leibniz properties of partial derivatives for (6). Case (7) exploits the chain rule and assignments and differential assignments for the fresh $y,y'$ to mimic partial derivatives. Equation (7) generalizes to functions $f$ of arity $n>1$, in which case $\cdot$ is the (definable) Euclidean scalar product.

$$I\nu[\![(f)']\!]=\sum_x\nu(x')\frac{\partial I[\![f]\!]}{\partial x}(\nu)=\sum_x\nu(x')\frac{\partial I(f)}{\partial x}(\nu)=0 \tag{3}$$

$$I\nu[\![(x)']\!]=\sum_y\nu(y')\frac{\partial I[\![x]\!]}{\partial y}(\nu)=\nu(x')=I\nu[\![x']\!] \tag{4}$$

$$I\nu[\![(\theta+\eta)']\!]=\sum_x\nu(x')\frac{\partial I[\![\theta+\eta]\!]}{\partial x}(\nu)=\sum_x\nu(x')\frac{\partial(I[\![\theta]\!]+I[\![\eta]\!])}{\partial x}(\nu)$$

$$= \sum_x \nu(x') \left( \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) + \frac{\partial I[\![\eta]\!]}{\partial x}(\nu) \right)$$
$$= \sum_x \nu(x') \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) + \sum_x \nu(x') \frac{\partial I[\![\eta]\!]}{\partial x}(\nu)$$
$$= I\nu[\![(\theta)']\!] + I\nu[\![(\eta)']\!] = I\nu[\![(\theta)' + (\eta)']\!] \tag{5}$$

$$I\nu[\![(\theta \cdot \eta)']\!] = \sum_x \nu(x') \frac{\partial I[\![\theta \cdot \eta]\!]}{\partial x}(\nu) = \sum_x \nu(x') \frac{\partial (I[\![\theta]\!] \cdot I[\![\eta]\!])}{\partial x}(\nu)$$
$$= \sum_x \nu(x') \left( I\nu[\![\eta]\!] \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) + I\nu[\![\theta]\!] \frac{\partial I[\![\eta]\!]}{\partial x}(\nu) \right)$$
$$= I\nu[\![\eta]\!] \sum_x \nu(x') \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) + I\nu[\![\theta]\!] \sum_x \nu(x') \frac{\partial I[\![\eta]\!]}{\partial x}(\nu)$$
$$= I\nu[\![(\theta)']\!] \cdot I\nu[\![\eta]\!] + I\nu[\![\theta]\!] \cdot I\nu[\![(\eta)']\!] = I\nu[\![(\theta)' \cdot \eta + \theta \cdot (\eta)']\!] \tag{6}$$

Proving that $\nu \in I[\![[y := \theta][y' := 1]\big((f(\theta))' = (f(y))' \cdot (\theta)'\big)]\!]$ requires $\omega \in I[\![(f(\theta))' = (f(y))' \cdot (\theta)']\!]$, i.e. that $I\omega[\![(f(\theta))']\!] = I\omega[\![(f(y))' \cdot (\theta)']\!]$, where $\omega$ agrees with state $\nu$ except that $\omega(y) = I\nu[\![\theta]\!]$ and $\omega(y') = 1$. This is equivalent to $I\nu[\![(f(\theta))']\!] = I\omega[\![(f(y))']\!] \cdot I\nu[\![(\theta)']\!]$ by Lemma 10 since $\nu = \omega$ on $\{y, y'\}^{\complement}$ and $y, y' \notin \mathsf{FV}(\theta)$ by assumption, so $y, y' \notin \mathsf{FV}((f(\theta))')$ and $y, y' \notin \mathsf{FV}((\theta)')$. The latter equation proves using the chain rule (Lemma 42) and a fresh variable $z$ when denoting $I[\![f]\!] \overset{\text{def}}{=} I(f)$ using Lemma 10:

$$I\nu[\![(f(\theta))']\!] = \sum_x \nu(x') \frac{\partial I[\![f(\theta)]\!]}{\partial x}(\nu) = \sum_x \nu(x') \frac{\partial (I[\![f]\!] \circ I[\![\theta]\!])}{\partial x}(\nu)$$
$$\overset{\text{chain}}{=} \sum_x \nu(x') \frac{\partial I[\![f]\!]}{\partial y}\big(I\nu[\![\theta]\!]\big) \cdot \frac{\partial I[\![\theta]\!]}{\partial x}(\nu)$$
$$= \frac{\partial I[\![f]\!]}{\partial y}\big(I\nu[\![\theta]\!]\big) \cdot \sum_x \nu(x') \frac{\partial I[\![\theta]\!]}{\partial x}(\nu) = \frac{\partial I[\![f]\!]}{\partial y}\big(I\nu[\![\theta]\!]\big) \cdot I\nu[\![(\theta)']\!]$$
$$= \frac{\partial I(f)}{\partial y}\big(I\nu[\![\theta]\!]\big) \cdot I\nu[\![(\theta)']\!] = \frac{\partial I(f)}{\partial z}\big(I\omega[\![y]\!]\big) \frac{\partial I[\![y]\!]}{\partial y}(\omega) \cdot I\nu[\![(\theta)']\!]$$
$$\overset{\text{chain}}{=} \frac{\partial (I(f) \circ I[\![y]\!])}{\partial y}(\omega) \cdot I\nu[\![(\theta)']\!] = \left( \frac{\partial I[\![f(y)]\!]}{\partial y}(\omega) \right) \cdot I\nu[\![(\theta)']\!]$$
$$= \left( \omega(y') \frac{\partial I[\![f(y)]\!]}{\partial y}(\omega) \right) \cdot I\nu[\![(\theta)']\!]$$
$$= \left( \sum_{x \in \{y\}} \omega(x') \frac{\partial I[\![f(y)]\!]}{\partial x}(\omega) \right) \cdot I\nu[\![(\theta)']\!]$$
$$= I\omega[\![(f(y))']\!] \cdot I\nu[\![(\theta)']\!] \tag{7}$$

□

*Proof of Lemma 39.* Let $\tilde{\varphi}$ be the desired instance of the axiom schema belonging to $\varphi$, that is, let $\tilde{\varphi}$ be obtained from $\varphi$ by uniformly replacing each quantifier symbol $C()$ by some formula, naïvely but consistently (same replacement for $C()$ in all places) and accordingly for program constants $a$. The proof follows a structural induction on $\varphi$ to show that there is

a uniform substitution $\sigma$ with $\mathrm{FV}(\sigma) = \emptyset$ such that $\sigma(\varphi) = \tilde{\varphi}$. The proof for formulas is by a mostly straightforward simultaneous induction with programs:

1. Consider quantifier symbol $C()$ of arity 0 and let $\tilde{\varphi}$ be the desired instance. Define $\sigma = \{C() \mapsto \tilde{\varphi}\}$, which has $\mathrm{FV}(\sigma) = \emptyset$, because it only substitutes quantifier symbols. Then $\sigma(C()) \equiv \sigma C() \equiv \tilde{\varphi}$. The substitution is admissible for all arguments, since there are none.
2. Consider $\phi \wedge \psi$ and let $\tilde{\phi} \wedge \tilde{\psi}$ be the desired instance (which has to have this shape to qualify as a schema instance). By induction hypothesis, there are uniform substitutions $\sigma, \tau$ with $\mathrm{FV}(\sigma) = \mathrm{FV}(\tau) = \emptyset$ such that $\sigma(\phi) = \tilde{\phi}$ and $\sigma(\psi) = \tilde{\psi}$. Then the union $\sigma \cup \tau$ of uniform substitutions $\sigma$ and $\tau$ is defined, because for all symbols $a$ of any syntactic category: if $a \in \sigma$ and $a \in \tau$, then $\sigma a = \tau a$ since all replacements are uniform, so the same replacement is used everywhere in $\phi \wedge \psi$ for the same symbol $a$. Consequently, $(\sigma \cup \tau)(\phi) = \sigma(\phi) = \tilde{\phi}$ and $(\sigma \cup \tau)(\psi) = \tau(\psi) = \tilde{\psi}$, because all symbols that are replaced are replaced uniformly everywhere so either do not occur in $\phi$ or are already handled by $\sigma$ in the same way (and likewise either do not occur in $\psi$ or are already handled by $\tau$). Finally, $\mathrm{FV}(\sigma \cup \tau) = \mathrm{FV}(\sigma) \cup \mathrm{FV}(\tau) = \emptyset$.
3. Case 2 generalizes to a general *uniform replacement argument*: the induction hypothesis and uniform replacement assumptions imply for each subexpression $\theta \circ \eta$ of $\varphi$ with any operator $\circ$ that the corresponding desired instance has to have the same shape $\tilde{\theta} \circ \tilde{\eta}$ and that there are uniform substitutions $\sigma, \tau$ with $\mathrm{FV}(\sigma) = \mathrm{FV}(\tau) = \emptyset$ such that their union $\sigma \cup \tau$ is defined and $(\sigma \cup \tau)(\theta \circ \eta) = \sigma(\theta) \circ \tau(\eta) = \tilde{\theta} \circ \tilde{\eta}$ and $\mathrm{FV}(\sigma \cup \tau) = \mathrm{FV}(\sigma) \cup \mathrm{FV}(\tau) = \emptyset$. This shows the cases $\phi \vee \psi$, $\phi \rightarrow \psi$, $\phi \leftrightarrow \psi$ and, after a moment's thought, also $\neg\phi$.
4. Consider $\forall x\, \phi$ with desired instance $\forall x\, \tilde{\phi}$, which has to have this shape. By induction hypothesis, there is a uniform substitution $\sigma$ with $\mathrm{FV}(\sigma) = \emptyset$ such that $\sigma(\phi) = \tilde{\phi}$. Thus, $\sigma(\forall x\, \phi) = \forall x\, \sigma(\phi) = \forall x\, \tilde{\phi}$, which is $\{x\}$-admissible because $\mathrm{FV}(\sigma) = \emptyset$.
5. The case $\exists x\, \phi$ is accordingly.
6. Consider $[\alpha]\phi$ with desired instance $[\tilde{\alpha}]\tilde{\phi}$. By induction hypothesis and the uniform replacement argument, there are uniform substitutions $\sigma, \tau$ such that $(\sigma \cup \tau)([\alpha]\phi) = [\sigma(\alpha)]\tau(\phi) = [\tilde{\alpha}]\tilde{\phi}$ which is admissible, because $\sigma \cup \tau$ is $\mathrm{BV}((\sigma \cup \tau)(\alpha))$-admissible for $[\alpha]\phi$ since $\mathrm{FV}(\sigma \cup \tau) = \emptyset$.
7. The case $\langle\alpha\rangle\phi$ is accordingly.

The proof for hybrid programs is by simultaneous induction with formulas, where most cases are in analogy to the previous cases, except:

1. Consider program constant $a$ with desired instance $\tilde{a}$. Then $\sigma = \{a \mapsto \tilde{a}\}$ has $\mathrm{FV}(\sigma) = \emptyset$ and satisfies $\sigma(a) = \sigma a = \tilde{a}$.
2. Consider the case $x' = \theta \,\&\, \psi$ with desired instance $x' = \tilde{\theta} \,\&\, \tilde{\psi}$, which has to have this shape. By induction hypothesis and uniform replacement argument, there are uniform substitutions $\sigma, \tau$ such that $(\sigma \cup \tau)(x' = \theta \,\&\, \psi) \equiv x' = \sigma(\theta) \,\&\, \tau(\psi) \equiv x' = \tilde{\theta} \,\&\, \tilde{\psi}$. Admissibility follows from $\mathrm{FV}(\sigma \cup \tau) = \emptyset$.
3. Consider the case $\alpha^*$ with desired instance $(\tilde{\alpha})^*$, which has to have this shape. By induction hypothesis, there is a uniform substitution $\sigma$ such that $\sigma(\alpha) \equiv \tilde{\alpha}$ and $\mathrm{FV}(\sigma) = \emptyset$. Then $\sigma(\alpha^*) \equiv (\sigma(\alpha))^* \equiv (\tilde{\alpha})^*$, which is $\mathrm{BV}(\sigma(\alpha))$-admissible since $\mathrm{FV}(\sigma) = \emptyset$.
4. The case $\alpha; \beta$ is similar and case $\alpha \cup \beta$ follows directly from the uniform replacement argument.

The corresponding result for axiomatic rules built from surjective dL formulas follows since surjective dL formulas can be instantiated by rule US to any instance, which, thus, continues to hold for the premises and conclusions in rule USR. □

*Proof of Theorem 40.* This proof refines the completeness proof for the axiom schemata of differential game logic [16] with explicit proofs of instantiability by US and USR. Write $\vdash_L \phi$ to indicate that dL formula $\phi$ can be derived in the dL proof calculus from valid $L$ formulas. Soundness follows from Theorem 38, so it remains to prove completeness. For every valid dL formula $\phi$ it has to be proved that $\phi$ can be derived from valid $L$ tautologies within the dL calculus: from $\vDash \phi$ prove $\vdash_L \phi$. The proof proceeds as follows: By propositional recombination, inductively identify fragments of $\phi$ that correspond to $\phi_1 \rightarrow \langle\alpha\rangle\phi_2$ or $\phi_1 \rightarrow [\alpha]\phi_2$ logically. Find structurally simpler formulas from which these properties can be derived in the dL calculus by uniform substitution instantiations, taking care that the resulting formulas are simpler than the original one in a well-founded order. Finally, prove that the original dL formula can be re-derived from the subproofs in the dL calculus by uniform substitution instantiations.

The first insight is that, with the rules MP and $\forall$ and (by Lemma 39, all) relevant instances of $\forall$i, $\forall\rightarrow$, $\mathrm{V}_\forall$ and real arithmetic, the dL calculus contains a complete axiomatization of first-order logic. Thus, all first-order logic tautologies can be used without further notice in the remainder of the proof. Furthermore, by Lemma 39, all instances of $\langle\cdot\rangle$, [$\cup$], [;], [$^*$], K, I can be proved by rule US in the dL calculus.

By appropriate propositional derivations, assume $\phi$ to be given in conjunctive normal form. Assume that negations are pushed inside over modalities using the dualities $\neg[\alpha]\phi \equiv \langle\alpha\rangle\neg\phi$ and $\neg\langle\alpha\rangle\phi \equiv [\alpha]\neg\phi$ that are provable by axiom $\langle\cdot\rangle$, and that negations are pushed inside over quantifiers using definitorial first-order equivalences $\neg\forall x\, \phi \equiv \exists x\, \neg\phi$ and $\neg\exists x\, \phi \equiv \forall x\, \neg\phi$. The remainder of the proof follows an induction on a well-founded partial order $\prec$ from previous work [16] induced on dL formulas by the lexicographic ordering of the overall structural complexity of the hybrid programs in the formula and the structural complexity of the formula itself, with the logic $L$ placed at the bottom of the partial order $\prec$. The base logic $L$ is considered of lowest complexity by relativity, because $\vDash F$ immediately implies $\vdash_L F$ for all formulas $F$ of $L$. The monotonicity rules derive from G, K, $\langle\cdot\rangle$ by Lemma 39 with a classical argument:

$$\text{(M)}\ \frac{p(\bar{x}) \rightarrow q(\bar{x})}{\langle a\rangle p(\bar{x}) \rightarrow \langle a\rangle q(\bar{x})} \qquad \text{(M}_{[\cdot]}\text{)}\ \frac{p(\bar{x}) \rightarrow q(\bar{x})}{[a]p(\bar{x}) \rightarrow [a]q(\bar{x})}$$

The proof follows the syntactic structure of dL formulas.

0. If $\phi$ has no hybrid programs, then $\phi$ is a first-order formula; hence provable by assumption (even decidable if in first-order real arithmetic [21], i.e. no uninterpreted symbols occur).
1. $\phi$ is of the form $\neg\phi_1$; then $\phi_1$ is first-order and quantifier-free, as negations are assumed to be pushed inside, so Case 0 applies.
2. $\phi$ is of the form $\phi_1 \wedge \phi_2$, then $\vDash \phi_1$ and $\vDash \phi_2$, so individually deduce simpler proofs for $\vdash_L \phi_1$ and $\vdash_L \phi_2$ by IH, which combine propositionally to a proof for $\vdash_L \phi_1 \wedge \phi_2$ using MP twice with the propositional tautology $\phi_1 \rightarrow (\phi_2 \rightarrow \phi_1 \wedge \phi_2)$.
3. The case where $\phi$ is of the form $\exists x\, \phi_2$, $\forall x\, \phi_2$, $\langle\alpha\rangle\phi_2$ or $[\alpha]\phi_2$ is included in Case 4 with $\phi_1 \equiv \mathit{false}$.
4. $\phi$ is a disjunction and—without loss of generality—has one of the following forms (otherwise use provable associativity and commutativity to reorder):

$$\begin{array}{l}\phi_1 \vee \langle\alpha\rangle\phi_2\\ \phi_1 \vee [\alpha]\phi_2\\ \phi_1 \vee \exists x\, \phi_2\\ \phi_1 \vee \forall x\, \phi_2.\end{array}$$

Let $\phi_1 \vee \langle\!|\alpha|\!\rangle\phi_2$ be a unified notation for those cases. Then, $\phi_2 \prec \phi$, since $\phi_2$ has less modalities or quantifiers. Likewise, $\phi_1 \prec \phi$ because $\langle\!|\alpha|\!\rangle\phi_2$ contributes one modality or quantifier to $\phi$ that is not part of $\phi_1$. When abbreviating the simpler formulas $\neg\phi_1$ by $F$ and $\phi_2$ by $G$, the validity $\models \phi$ yields $\models \neg F \vee \langle\!|\alpha|\!\rangle G$, so $\models F \to \langle\!|\alpha|\!\rangle G$, from which the remainder of the proof inductively derives

$$\vdash_L F \to \langle\!|\alpha|\!\rangle G. \tag{9}$$

The proof of (9) is by structural induction on $\langle\!|\alpha|\!\rangle$. This proof focuses on the quantifier and [] cases, because most $\langle\rangle$ cases derive by axiom $\langle\cdot\rangle$ with Lemma 39 from the [] equivalences.

(a) If $\langle\!|\alpha|\!\rangle$ is the operator $\forall x$ then $\models F \to \forall x\, G$, where $x$ can be assumed not to occur in $F$ by a bound variable renaming. Hence, $\models F \to G$. Since $G \prec \forall x\, G$, because it has less quantifiers, also $(F \to G) \prec (F \to \forall x\, G)$, hence $\vdash_L F \to G$ is derivable by IH. Then, $\vdash_L F \to \forall x\, G$ derives with Lemma 39 by generalization rule $\forall$, since $x$ does not occur in $F$:

$$\mathrm{V}_\forall\,\dfrac{\forall_{\to}\,\dfrac{\forall\,\dfrac{F \to G}{\forall x\,(F \to G)}}{\forall x\, F \to \forall x\, G}}{F \to \forall x\, G}$$

The instantiations succeed by the remark after Lemma 39 using for $\mathrm{V}_\forall$ that $x \notin \mathrm{V}(F)$. The formula $F \to \forall x\, G$ is even decidable if in first-order real arithmetic [21]. The remainder of the proof concludes $(F \to \psi) \prec (F \to \phi)$ from $\psi \prec \phi$ without further notice. The operator $\forall y$ can be obtained correspondingly by uniform renaming.

(b) If $\langle\!|\alpha|\!\rangle$ is the operator $\exists x$ then $\models F \to \exists x\, G$. If $F$ and $G$ are $L$ formulas, then, since $L$ is closed under first-order connectives, so is the valid formula $F \to \exists x\, G$, which is, then, provable by IH and even decidable if in first-order real arithmetic [21]. Otherwise, $F$, $G$ correspond to $L$ formulas by expressiveness of $L$, which implies the existence of an $L$ formula $G^\flat$ such that $\models G^\flat \leftrightarrow G$. Since $L$ is closed under first-order connectives [16], the valid formula $F \to \exists x\,(G^\flat)$ is provable by IH, because $(F \to \exists x\,(G^\flat)) \prec (F \to \exists x\, G)$ since $G^\flat \in L$ while $G \notin L$. Now, $\models G^\flat \leftrightarrow G$ implies $\models G^\flat \to G$, which is derivable by IH, because $(G^\flat \to G) \prec \phi$ since $G^\flat$ is in $L$. From $\vdash_L G^\flat \to G$, the derivable dual of axiom $\forall\to$, $(\forall x\,(p(x) \to q(x)) \to (\exists x\, p(x) \to \exists x\, q(x)))$, derives $\vdash_L \exists x\,(G^\flat) \to \exists x\, G$, which combines with $\vdash_L F \to \exists x\,(G^\flat)$ essentially by rule MP to $\vdash_L F \to \exists x\, G$.

$$\mathrm{MP}\,\dfrac{F \to \exists x\,(G^\flat) \qquad \forall_{\to}\,\dfrac{\forall\,\dfrac{G^\flat \to G}{\forall x\,(G^\flat \to G)}}{\exists x\,(G^\flat) \to \exists x\, G}}{F \to \exists x\, G}$$

The instantiations succeed by Lemma 39 and its subsequent remark.

(c) $\models F \to \langle x' = \theta\rangle G$ implies $\models F \to (\langle x' = \theta\rangle G^\flat)^\flat$, which is derivable by IH, as $(F \to (\langle x' = \theta\rangle G^\flat)^\flat) \prec \phi$ since $(\langle x' = \theta\rangle G^\flat)^\flat$ is in $L$. $L$ is differentially expressive, so $\vdash_L \langle x' = \theta\rangle G^\flat \leftrightarrow (\langle x' = \theta\rangle G^\flat)^\flat$ is provable. Hence $\vdash_L F \to \langle x' = \theta\rangle G^\flat$ derives by propositional congruence. Now $G^\flat \to G$ is simpler (since $G^\flat$ is in $L$) so derivable by IH, so $\langle x' = \theta\rangle G^\flat \to \langle x' = \theta\rangle G$ derives by M. Together, both derive $\vdash_L F \to \langle x' = \theta\rangle G$ propositionally.

(d) $\models F \to [x' = \theta]G$ implies $\models F \to \neg\langle x' = \theta\rangle\neg G$. Thus, $\models F \to \neg(\langle x' = \theta\rangle\neg G^\flat)^\flat$, which is derivable by IH, because $(F \to \neg(\langle x' = \theta\rangle\neg G^\flat)^\flat) \prec \phi$ as $(\langle x' = \theta\rangle\neg G^\flat)^\flat$ is in $L$. Since $L$ is differentially expressive, $\vdash_L \langle x' = \theta\rangle\neg G^\flat \leftrightarrow (\langle x' = \theta\rangle\neg G^\flat)^\flat$ is provable, so $\vdash_L F \to \neg\langle x' = \theta\rangle\neg G^\flat$ derives from $\vdash_L F \to \neg(\langle x' = \theta\rangle\neg G^\flat)^\flat$ by propositional congruence. Axiom $\langle\cdot\rangle$, thus, derives $\vdash_L F \to [x' = \theta]G^\flat$ with Lemma 39. Now $G^\flat \to G$ is simpler (as $G^\flat$ is in $L$) so derivable by IH, so $[x' = \theta]G^\flat \to [x' = \theta]G$ derives by M. Together, both derive $\vdash_L F \to [x' = \theta]G$ propositionally.

(e) $\models F \to [x' = \theta \,\&\, \psi]G$, then this formula has an equivalent [16, Lemma 3.4] without evolution domains which can be used as a definitorial abbreviation to conclude this case. Similarly for $\models F \to \langle x' = \theta \,\&\, \psi\rangle G$.

(f) $\models F \to [y := \theta]G$ then this formula can be proved, using a fresh variable $x \notin \mathrm{V}(\theta) \cup \mathrm{V}(G)$, with the following derivation by bound variable renaming (rule BR), in which $G\frac{x}{y}$ is the result of uniformly renaming $y$ to $x$ in $G$

$$\cfrac{\cfrac{F \to \forall x\,(x = \theta \to G\frac{x}{y})}{F \to [x := \theta]G\frac{x}{y}}\,[:=]_=}{F \to [y := \theta]G}\,\mathrm{BR}$$

using the following equational form of the assignment axiom [:=]

$$([:=]_=)\quad [x := f]p(\bar{x}) \leftrightarrow \forall x\,(x = f \to p(\bar{x}))$$

The above proof only used equivalence transformations, so its premise is valid iff its conclusion is, which it is by assumption. The assumption, thus, implies $\models F \to \forall x\,(x = \theta \to G\frac{x}{y})$. Since $(F \to \forall x\,(x = \theta \to G\frac{x}{y})) \prec (F \to [y := \theta]G)$, because there are less hybrid programs, $\vdash_L F \to \forall x\,(x = \theta \to G\frac{x}{y})$ by IH. The above proof, thus, derives $\vdash_L F \to [y := \theta]G$.

The equational assignment axiom $[:=]_=$ above can either be adopted as an axiom in place of [:=]. Or it can be derived from axiom [:=] with the uniform substitution $\sigma = \{q(\cdot) \mapsto p(\cdot, X)\}$ when splitting the variables $\bar{x}$ into the variable $x$ and the other variables $X$ such that $x \notin X$:

$$\cfrac{\cfrac{\cfrac{*}{q(f) \leftrightarrow \forall x\,(x = f \to q(x))}\,\mathrm{FOL}}{[x := f]q(x) \leftrightarrow \forall x\,(x = f \to q(x))}\,[:=]}{[x := f]p(x, X) \leftrightarrow \forall x\,(x = f \to p(x, X))}\,\mathrm{US}}{[x := f]p(\bar{x}) \leftrightarrow \forall x\,(x = f \to p(\bar{x}))}$$

It only remains to be shown that $[:=]_=$ can be instantiated as indicated in the above proof. This follows from Lemma 39 with the additional observation that the required uniform substitution $\{f \mapsto \theta\}$ of function symbol $f$ of arity 0 without argument $\bar{x}$ will not cause a clash during US, because the only bound variable $x$ in $[:=]_=$ is not free in the substitution since $x \notin \mathrm{V}(\theta)$.

Other proofs involving stuttering and renaming are possible. Direct proofs of $F \to [y := \theta]G$ by axiom [:=] are possible if the substitution is admissible.

(g) $\models F \to [?\psi]G$ implies $\models F \to (\psi \to G)$. Since $(\psi \to G) \prec [?\psi]G$, because it has less modalities, $\vdash_L F \to (\psi \to G)$ is derivable by IH. Hence, with the remark after Lemma 39, axiom [?] instantiates to $[?\psi]G \leftrightarrow (\psi \to G)$, so derives

$\vdash_L F \to [?\psi]G$ by propositional congruence, which is used without further notice subsequently.

(h) $\vDash F \to [\beta \cup \gamma]G$ implies $\vDash F \to [\beta]G \wedge [\gamma]G$. Since $[\beta]G \wedge [\gamma]G \prec [\beta \cup \gamma]G$, because, even if the propositional and modal structure increased, the structural complexity of both hybrid programs $\beta$ and $\gamma$ is smaller than that of $\beta \cup \gamma$ (formula $G$ did not change), $\vdash_L F \to [\beta]G \wedge [\gamma]G$ is derivable by IH. Hence, with Lemma 39, axiom [∪] instantiates to $[\beta \cup \gamma]G \leftrightarrow [\beta]G \vee [\gamma]G$, so derives $\vdash_L F \to [\beta \cup \gamma]G$ by propositional congruence.

(i) $\vDash F \to [\beta;\gamma]G$, which implies $\vDash F \to [\beta][\gamma]G$. Since $[\beta][\gamma]G \prec [\beta;\gamma]G$, because, even if the number of modalities increased, the overall structural complexity of the hybrid programs decreased because there are less sequential compositions, $\vdash_L F \to [\beta][\gamma]G$ is derivable by IH. Hence, with Lemma 39, $\vdash_L F \to [\beta;\gamma]G$ derives by axiom [;] by propositional congruence.

(j) $\vDash F \to [\beta^*]G$ can be derived by induction as follows. Formula $[\beta^*]G$, which expresses that all numbers of repetitions of $\beta^*$ satisfy $G$, is an inductive invariant of $\beta^*$, because $[\beta^*]G \to [\beta][\beta^*]G$ is valid, even provable by [*]. Thus, its equivalent $L$ encoding is also an inductive invariant:

$$\varphi \equiv ([\beta^*]G)^\flat.$$

Then $F \to \varphi$ and $\varphi \to G$ are valid (zero repetitions are possible), so derivable by IH, since $(F \to \varphi) \prec \phi$ and $(\varphi \to G) \prec \phi$ hold, because $\varphi$ is in $L$. As above, $\varphi \to [\beta]\varphi$ is valid, and thus derivable by IH, since $\beta$ has less loops than $\beta^*$. By $\mathrm{M}_{[\cdot]}$ as well as rule ind (from $p(\bar{x}) \to [a]p(\bar{x})$ conclude $p(\bar{x}) \to [a^*]p(\bar{x})$), which derives from I, G by Lemma 39, the respective rules can be instantiated by Lemma 39 and the resulting derivations combine by MP:

$$\dfrac{F \to \varphi \qquad \dfrac{\dfrac{\varphi \to [\beta]\varphi}{\varphi \to [\beta^*]\varphi}\,\text{ind} \qquad \dfrac{\varphi \to G}{[\beta^*]\varphi \to [\beta^*]G}\,\mathrm{M}_{[\cdot]}}{\varphi \to [\beta^*]G}\,\text{MP}}{F \to [\beta^*]G}\,\text{MP}$$

(k) $\vDash F \to \langle\beta^*\rangle G$. Let $x$ be the vector of free variables $\mathrm{FV}(\langle\beta^*\rangle G)$. Since $\langle\beta^*\rangle G$ is a least pre-fixpoint [16], for all dL formulas $\psi$ with $\mathrm{FV}(\psi) \subseteq \mathrm{FV}(\langle\beta^*\rangle G)$:

$$\vDash \forall x\, (G \vee \langle\beta\rangle\psi \to \psi) \to (\langle\beta^*\rangle G \to \psi)$$

In particular, this holds for a fresh predicate symbol $p$ with arguments $x$:

$$\vDash \forall x\, (G \vee \langle\beta\rangle p(x) \to p(x)) \to (\langle\beta^*\rangle G \to p(x))$$

Using $\vDash F \to \langle\beta^*\rangle G$, this implies

$$\vDash \forall x\, (G \vee \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))$$

As $(\forall x\, (G \vee \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))) \prec \phi$, because, even if the formula complexity increased, the structural complexity of the hybrid programs decreased, since $\phi$ has one more loop, this fact is derivable by IH:

$$\vdash_L \forall x\, (G \vee \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))$$

The uniform substitution $\sigma = \{p(x) \mapsto \langle\beta^*\rangle G\}$ is admissible since $\mathrm{FV}(\sigma) = \emptyset$ as $\langle\beta^*\rangle G$ has free variables $x$. Since, furthermore, $p \notin \Sigma(F) \cup \Sigma(G) \cup \Sigma(\beta)$, US derives:

$$\text{US}\,\frac{\forall x\,(G \vee \langle\beta\rangle p(x) \to p(x)) \to (F \to p(x))}{\forall x\,(G \vee \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G) \to (F \to \langle\beta^*\rangle G)}$$

The dual $\langle a^*\rangle p(\bar{x}) \leftrightarrow p(\bar{x}) \vee \langle a\rangle\langle a^*\rangle p(\bar{x})$ resulting from axiom [*] with axiom $\langle\cdot\rangle$ by Lemma 39 continues this derivation by Lemma 39:

$$\text{MP}\,\frac{\forall x\,(G \vee \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G) \to (F \to \langle\beta^*\rangle G) \qquad \forall\,\dfrac{[*],\langle\cdot\rangle\,\dfrac{*}{G \vee \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G}}{\forall x\,(G \vee \langle\beta\rangle\langle\beta^*\rangle G \to \langle\beta^*\rangle G)}}{F \to \langle\beta^*\rangle G}$$

Observe that rule ∀ (and MP) instantiates as needed with USR by Lemma 39.

This concludes the derivation of (9), because all operators $\langle\!\langle\alpha\rangle\!\rangle$ for the form (9) have been considered. From (9), which is $\vdash_L \neg\phi_1 \to \langle\!\langle\alpha\rangle\!\rangle\phi_2$, hence, $\vdash_L \phi_1 \vee \langle\!\langle\alpha\rangle\!\rangle\phi_2$ derives propositionally.

This completes the proof of completeness (Theorem 40), because all syntactical forms of dL formulas have been covered. □

## References


1. Church, A.: A formulation of the simple theory of types. J. Symb. Log. **5**(2), 56–68 (1940)
2. Church, A.: Introduction to Mathematical Logic, vol. I. Princeton University Press, Princeton, NJ (1956)
3. Cimatti, A., Roveri, M., Tonetta, S.: HRELTL: a temporal logic for hybrid systems. Inf. Comput. **245**, 54–71 (2015). doi:10.1016/j.ic.2015.06.006
4. Davoren, J.M., Nerode, A.: Logics for hybrid systems. IEEE **88**(7), 985–1010 (2000)
5. Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. J. Autom. Reas. **31**(1), 33–72 (2003)
6. Fulton, N., Mitsch, S., Quesel, J.D., Völp, M., Platzer, A.: KeYmaera X: an axiomatic tactical theorem prover for hybrid systems. In: Felty, A., Middeldorp, A. (eds.) CADE, LNCS, vol. 9195, pp. 527–538. Springer, Berlin (2015). doi:10.1007/978-3-319-21401-6_36
7. Harel, D., Kozen, D., Tiuryn, J.: Dynamic Logic. MIT Press, Cambridge, MA (2000)
8. Henkin, L.: Banishing the rule of substitution for functional variables. J. Symb. Log. **18**(3), 201–208 (1953)
9. Hughes, G.E., Cresswell, M.J.: A New Introduction to Modal Logic. Routledge, London (1996)
10. Liu, J., Lv, J., Quan, Z., Zhan, N., Zhao, H., Zhou, C., Zou, L.: A calculus for hybrid CSP. In: Ueda, K. (ed.) APLAS, LNCS, vol. 6461, pp. 1–15. Springer, Berlin (2010). doi:10.1007/978-3-642-17164-2_1
11. Pfenning, F.: Logical frameworks. In: Robinson, J.A., Voronkov, A. (eds.) Handbook of Automated Reasoning, pp. 1063–1147. MIT Press, Cambridge, MA (2001)
12. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas. **41**(2), 143–189 (2008). doi:10.1007/s10817-008-9103-8
13. Platzer, A.: Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. **20**(1), 309–352 (2010). doi:10.1093/logcom/exn070
14. Platzer, A.: The complete proof theory of hybrid systems. In: LICS, pp. 541–550. IEEE (2012). doi:10.1109/LICS.2012.64
15. Platzer, A.: The structure of differential invariants and differential cut elimination. Log. Meth. Comput. Sci. **8**(4), 1–38 (2012). doi:10.2168/LMCS-8(4:16)2012
16. Platzer, A.: Differential game logic. ACM Trans. Comput. Log. **17**(1), 1:1–1:51 (2015). doi:10.1145/2817824
17. Platzer, A.: Differential Hybrid Games. CoRR arXiv:1507.04943 (2015)
18. Platzer, A.: A uniform substitution calculus for differential dynamic logic. In: Felty, A., Middeldorp, A. (eds.) CADE, LNCS, vol. 9195, pp. 467–481. Springer, Berlin (2015). doi:10.1007/978-3-319-21401-6_32
19. Platzer, A., Quesel, J.D.: KeYmaera: a hybrid theorem prover for hybrid systems. In: Armando, A., Baumgartner, P., Dowek, G. (eds.) IJCAR, LNCS, vol. 5195, pp. 171–178. Springer, Berlin (2008). doi:10.1007/978-3-540-71070-7_15
20. Rice, H.G.: Classes of recursively enumerable sets and their decision problems. Trans. AMS **89**, 25–59 (1953)

21. Tarski, A.: A Decision Method for Elementary Algebra and Geometry, 2nd edn. University of California Press, Berkeley (1951)
22. Walter, W.: Analysis 1. Springer, Berlin (1985)
23. Walter, W.: Analysis 2, 4th edn. Springer, Berlin (1995)
24. Walter, W.: Ordinary Differential Equations. Springer, Berlin (1998)